

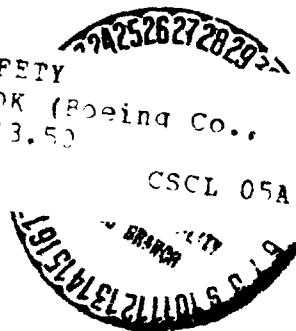
(NASA-CR-131886) SYSTEM SAFETY
ENGINEERING ANALYSIS HANDBOOK (Boeing Co.,
Seattle, Wash.) 230 D HC \$13.50

N73-22913

CSCL 05A

G3/34

Unclass
17538



THE **BOEING** COMPANY

REV LTR

CODE IDENT. NO. 81205

NUMBER D2-119062-1

TITLE: System Safety Engineering Analysis Handbook

FOR LIMITATIONS IMPOSED ON THE USE OF THE INFORMATION
CONTAINED IN THIS DOCUMENT AND ON THE DISTRIBUTION
OF THIS DOCUMENT, SEE LIMITATIONS SHEET.

MODEL _____ CONTRACT NASW1650

ISSUE NO. _____ ISSUED TO: _____

TIE System Safety
PREPARED BY *Jerry E. Dams*
Jerry E. Dams
SUPERVISED BY *Robert C. Har*
Robert C. Har
APPROVED BY *Thomas G. Goss*
Thomas G. Goss
APPROVED BY *Edgar F. McIntosh*
Edgar F. McIntosh

SHEET 1

ABSTRACT

This document sets forth the basic requirements and guidelines for the preparation of System Safety Engineering Analysis. It discusses the philosophy of System Safety and details the various analytic methods available to the engineering profession. Appendices provide a textbook description of each of the methods. The document is a handbook and should be used as a source of information and guidance.

KEY WORDS

System Engineering Analysis
System Safety Engineering Analyses
Fault Tree Analysis
Failure Mode and Effects Analysis
Gross Hazards Analysis
Operations Analysis
Fracture Mechanics Analysis

USE FOR TYPEWRITTEN MATERIAL ONLY

TABLE OF CONTENTS

<u>Paragraph</u>		<u>Page</u>
	Abstract and Key Words	2
	Table of Contents	3
	List of Figures	7
	Preface	8

SECTION I - INTRODUCTION

1.0	Introduction	1-1
1.1	Purpose	1-1
1.2	Scope	1-1
1.3	Objectives	1-2
1.4	System Safety Analysis Philosophy	1-2
1.5	NASA Safety Direction	1-2

SECTION II - SELECTION OF METHOD

2.0	Selection of Method	2-1
2.1	Method Selection Matrix	2-5

SECTION III - DATA INPUTS

3.0	Data Inputs	3-1
3.1	Types of Data	3-1
3.1.1	System Function and Description	3-1
3.1.2	System Environment	3-1
3.1.3	Failure Data	3-2
3.1.4	System Simulation Data	3-3
3.1.5	Other Studies	3-3
3.1.6	Sources of Data	3-3
3.1.6.1	Data Generating Organizations	3-3
3.1.6.2	Data Storing Organizations	3-6

USE FOR TYPEWRITTEN MATERIAL ONLY

<u>Paragraph</u>	<u>SECTION IV - ANALYTICAL METHODS</u>	<u>Page</u>
4.0	Analytical Methods	4-1
4.1	Gross Hazards Analysis	4-2
4.1.1	Summary Description of Technique	4-2
4.1.2	Applications of Gross Hazards Analysis	4-2
4.1.2.1	Priorities and Ground Rules	4-2
4.1.2.2	Design Control Criteria	4-3
4.1.2.3	Implementation	4-3
4.1.3	Input Data Required for Gross Hazards Analysis	4-3
4.1.4	Gross Hazards Analysis Procedure	4-3
4.2	Operations Safety Analysis	4-5
4.2.1	Summary Description of Technique	4-5
4.2.2	Application of Operations Safety Analysis	4-5
4.2.3	Input Data Required for Operations Safety Analysis	4-5
4.2.4	Operations Safety Analysis Procedure	4-5
4.2.4.1	Operations and Test Safety Analysis (OSA-I)	4-5
4.2.4.2	Operations Safety Research (OSA-II)	4-6
4.2.4.3	Human Error Prediction Techniques	4-6
4.3	Fault Tree Analysis	4-7
4.3.1	Summary Description of Technique	4-7
4.3.2	Applications of Fault Tree	4-9
4.3.3	Input Data Requirements for Fault Tree Analysis	4-9
4.3.3.1	System Function and Description	4-9
4.3.3.2	System Environment	4-10
4.3.3.3	Failure Data	4-10
4.3.3.4	Other Studies	4-11
4.3.4	Fault Tree Procedure	4-12

USE FOR TYPEWRITTEN MATERIAL ONLY

<u>Paragraph</u>	<u>SECTION IV - ANALYTICAL METHODS (Continued)</u>	<u>Page</u>
4.4	Fracture Mechanics Assessment	4-20
4.4.1	Summary Description of Techniques	4-20
4.4.2	Application of Fracture Mechanics Assessment	4-21
4.4.3	Input Data Requirements for Fracture Mechanics	4-21
4.4.4	Summary Description of Fracture Mechanics Assessment	4-22
4.4.4.1	Critical Flaw Sizes	4-22
4.4.4.2	Failure Mode Analysis	4-22
4.4.4.3	Allowable Stress Intensities	4-22
4.4.4.4	Allowable Flaws	4-23
4.4.4.5	Design Deviations	4-24
4.4.4.6	Nondestructive Inspection	4-24
4.4.4.7	Proof Test Procedures	4-24
4.4.4.7.1	Test Temperature	4-24
4.4.4.7.2	Test Fluids	4-24
4.4.4.7.3	Pressurization and Hold Times	4-25
4.4.4.7.4	Depressurization Time	4-25
4.4.4.7.5	Multiple Cycles	4-25
4.4.4.8	Combined Loads	4-25
4.4.4.9	Proof Test Inspection	4-26
4.5	Failure Mode, Effects, and Criticality Analysis	4-27
4.5.1	Summary Description of Technique	4-27
4.5.2	Application of FMECA	4-27
4.5.3	Input Data for FMECA	4-27
4.5.4	Procedure for FMECA	4-27

<u>Paragraph</u>		<u>Page</u>
	<u>SECTION V - REFERENCES</u>	
5.0	References	5-1
	<u>SECTION VI - DEFINITIONS</u>	
6.0	Definitions	6-1
Appendices		
	Appendix A Gross Hazards Analysis	A-001
	Appendix B Operations Safety Analysis	B-001
	Appendix C Fault Tree Analysis	C-001
	Appendix D Fracture Mechanics Assessment	D-001
	Appendix E Failure Mode, Effect and Criticality Analysis	E-001
	Limitations	1001
	Active Sheet Record	1002
	Revisions	1005

USE FOR TYPEWRITTEN MATERIAL ONLY

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Section</u>	<u>Page</u>
2-1	Study Areas	2	2-6
3-1	Input Data Requirements	3	3-10
4-1	Example Of A System	4	4-15
4-2	Simple Fault Tree	4	4-16
4-3	Expanded Fault Tree	4	4-18

USE FOR TYPEWRITTEN MATERIAL ONLY

PREFACE

This document, developed for the Director of Safety (KSC-SF) at the John F. Kennedy Space Center, is a handbook for the preparation of System Safety Engineering Analyses. It provides a general overview of system elements which are possible subjects for system safety studies, and suggests recommended methods of analysis for the various study areas and types of safety problems that may arise. The kind and form of output data and information which safety studies should provide are identified. Section 4 provides a summary of the basic methods of analysis and assessment; these discussions are amplified in the appendices for those who require more detail regarding suitable applications, data requirements, background and theory of each method, and the type of conclusions that each method is capable of providing. Credit for much of the material in this handbook is due the authors of the references in Section 5, since these provided much of the information contained herein.

USE FOR TYPEWRITTEN MATERIAL ONLY

NUMBER 02-119062-1
REV LTR

THE **ENGINEERING** COMPANY

USE FOR TYPEWRITTEN MATERIAL ONLY

SECTION I

INTRODUCTION

1.0 INTRODUCTION

Engineering development of a system requires systematic identification and solution of safety problems which arise from hazard potentials in the system. This process of identification and solution frequently requires system safety engineering analysis of specific systems and functions. There are a variety of methods and techniques that have been developed for, or are particularly apt to system safety study. These techniques enable the performance of system safety engineering analyses, and when integrated with total system engineering, contribute to equipment designs and operations which satisfy system safety requirements without compromising total system performance.

1.1 PURPOSE

The purpose of this document is to guide engineering specialists in the conduct of system safety engineering studies, and to provide criteria for the control of such studies in a cost effective manner.

In many projects, lack of early planning of system safety is the principal reason for the lack of true cost effectiveness in system safety. Historically new systems have been conceived for a primary mission and excluded secondary considerations such as safety, and reliability. There is generally little or no budgetary consideration given to the safety aspect of systems engineering in the conceptual stage. During the developmental and early operational phase most safety problems occur and are solved by "brinkmanship". That is, allowing them to become potentially serious problems, and then forging a fix for each. This approach lacks the unity of concept fundamental to good cost effectiveness.

Safety engineering after-the-fact proves to be costly, issues become confused and often the fix is abandoned due to trade-offs against schedule impact. This pendulum of unmodulated under-awareness to the problem and over-reaction can be controlled by the application of sound systems safety engineering during the conceptual or developmental phase.

1.2 SCOPE

This document provides a general overview of system elements or functions which are possible subjects for system safety study. It identifies information and output data that a safety study should provide in order to support management decisions with respect to system safety. Most important, it identifies and describes a variety of analytic techniques which are applicable to system safety problems. For each technique described, there is a discussion of suitable applications, input data requirements, operational steps in application, and the kind and quality of conclusions that may be drawn.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.2 (Continued)

Selected technical references are cited and technical appendices are included to identify or provide more detailed information for the user.

1.3 OBJECTIVES

The objective of this document is to provide guidelines for system safety engineering analysis, that will allow NASA to achieve standardization and uniformity of the overall approach to "safety" by its various support contractors.

This document also provides the engineering analyst with a selection of analytic tools, with instruction in their application, to facilitate the requirement of paragraph 1.5, by use of the techniques defined in Section 4.

1.4 SYSTEM SAFETY ANALYSIS PHILOSOPHY

Operational systems have and continue to have safety deficiencies inadvertently designed into them. The best way to resolve safety hazards is to design them out of the system. This may be achieved by conducting a thorough system safety analysis considering the possible trade-offs between various design alternatives. The philosophy dictating these analyses usually takes one of three approaches. The first approach asks the question: What degree of safety can be achieved from the minimum expense? The second: What maximum degree of safety can be achieved for a preselected expenditure? The third: What minimum expense is required to achieve a preselected safety level? With the third approach, caution must be exercised for it is possible that the most effective course of action provides a higher level of safety at a lower expense than the preselected safety level.

Inherent in the role of system safety is the responsibility of properly identifying and eliminating accident causes before they occur. It is a fact that behind most accidents there is a cause that can be identified and eliminated.

1.5 NASA SAFETY DIRECTION

The Office of Manned Space Flight (CMSF) has issued guidelines concerning the application of system safety principles to all manned space flight programs. The following is an extract from a letter, Subject: Implementation and Conduct of NASA System Safety Activities, dated July 24, 1968, and signed by the Director of Safety (DY):

"This is to communicate the desired approach in the conduct of system safety activities and to clearly delineate the results expected.

1.5 (Continued)

PURPOSE

"The purpose of system safety activities (like all safety activities) is the avoidance of injury to people and the avoidance of property loss (including flight hardware) to the maximum practical extent.

BASIC APPROACH

"Similar to other NASA safety activities, system safety requires a basic approach as follows:

1. Know the hazardous characteristics of the system (including the total environment). Specifically, this means hazards to people and property (including flight hardware).
2. Eliminate, insofar as possible, these hazards. If the hazards cannot be eliminated, take all practical steps to control them. These steps include both hardware and software considerations.
3. Identify the risks remaining as inherent in the system, its processing and its operation either in (1) normal modes or (2) out of tolerance modes brought about by failures or combinations of failures. These risks are the risks to people and property (including flight hardware).
4. Assure that the knowledge of residual risks identified is applied to the programmatic decision-making process.
5. Recognize that the management responsibility for achieving system safety flows along program organizational lines.
6. Bear in mind that the desired results from system safety activities are the minimizing of risks to the maximum practical extent and the application of the knowledge of these risks to management decisions. Also, assure an understanding at all management levels as to the risks being incurred by testing, transporting or operating the system or portions of the system.

all systems processing activities, through conduct of

USE FOR TYPEWRITTEN MATERIAL ONLY

1.5 (Continued)

WHERE SYSTEM SAFETY ACTIVITIES ARE REQUIRED

"System safety activities are required in all NASA space hardware programs, manned and unmanned, to assure protection of people and property from system flight hardware effects from design inception, through all systems processing activities, through conduct of the mission and including post-mission activities insofar as hazards arising from the mission may require.

WHERE SYSTEM SAFETY ACTIVITIES ARE SUGGESTED

"The philosophy, techniques and tools of the system safety approach are recommended, as applicable in: complicated industrial safety situations, complex laboratory operations, aircraft research, and other research activities.

WHY THE SYSTEM SAFETY APPROACH

"The reason for an organized NASA system safety approach include the following:

1. The complexity of systems, subsystems and components under extreme and complex conditions of environment and application. The inherent complexity of the NASA flight hardware systems demands analytical techniques of considerable sophistication in order to achieve problem identification and solution.
2. The need to fix considerable attention on the safety considerations arising out of total systems effects, where such effects cannot be discovered when considering portions of the system independently.
3. The subtleties inherent in the dynamic characteristics of flight hardware systems.
4. The need to assure that the safety aspects of the mission under normal conditions and under mission failure conditions are adequate.
5. The need to assure that system safety measures at all steps leading up to and after the mission are adequate.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.5 (Continued)

HOW TO IMPLEMENT SYSTEM SAFETY ACTIVITIES

"Successful and, therefore, satisfactory conduct of system safety activities include the following points of approach:

1. Personnel assigned in system safety work are to be --
 - a. Qualified to conduct the work
 - b. Assigned, exclusively, to the system safety mission
 - c. Organizationally placed to assure effectiveness.
2. Analytical techniques appropriate to the situation are to be use.
3. System safety is to take advantage of all useful inputs."

It is quite obvious from the above quotation that NASA management recognizes the need for a systematic analytic approach to system safety engineering. This document attempts to formalize the KSC-SF implementaion of the above requirements.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

SECTION II

SELECTION OF METHOD

2.0

SELECTION OF METHOD

The system which confronts the analyst may vary considerably in complexity from one assessment to the next. Whether the scope of analysis encompasses an entire manned spaceflight center such as KSC, or whether it is limited to one component such as a valve or relay, the "system" approach is equally valid. The safe development and use of a system involves many managerial, engineering, manufacturing and operational disciplines, regardless of whether that system is a complete launch facility or an individual device used on that facility. Application of the systems approach assures that the requirements and objectives of the system "user" will be realized in the safest and most economical manner the state of technology will allow. The usefulness of the systems approach increases as the complexity of the problem to be solved increases. Therefore, KSC Safety management must select from among the various methods of system analysis available that which is required to satisfy the safety problem posed.

For example, the question may be asked, "What is the numerical probability that death will be incurred by operational personnel during all phases of assembly, test and checkout of the Space Vehicle for Mission X?" Answering that question requires a complex detailed quantitative analysis spanning many facilities and agencies.

Another example: A question of quite different character may be asked of the system safety analyst. "What specific risks to equipment and men must be avoided during the operation of hypergolic propellant transfer unit, number abc, during Spacecraft loading at the launch facility?" This question is not only much smaller in scope and complexity, but suggests a qualitative analysis. Relative probabilities may be useful for assessment formulation and critical risk identification, but the absolute statistical analysis required to answer the question in the first example is not necessary or even desirable because of the undesirable costs of "over analysis."

When system safety engineers are required to perform analyses at the same time that the system design is developing, the system managers may not provide specific questions to be answered, but will still require a complete assessment of the level of safety allowed by the proposed design. Maximum benefit is derived from analyses conducted during design phases because alternatives and trade-offs can be compared for optimal safety, and the best solution can be incorporated in the final system design without expensive modification to the completed system.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 (Continued)

The degree of system design definition available to the analyst may dictate the method of analysis. It is impossible to construct a Failure Mode and Effects Analysis (FMEA), or much of a fault tree when only the basic scheme for the system is known. A Gross Hazards Analysis, as defined in paragraph 4.1, completed in time may demonstrate that some other design concept is essential if a high degree of safety is to be obtained. Gross Hazards Analysis provides a quick method for the system safety engineer to apply experience from detailed analyses conducted for other systems which have a reasonable degree of similarity to the proposed system design concept.

The extent and detail of the safety analysis required early in the program is largely dependent on the complexity of the system to be analyzed and the desired accuracy of the answer, and this will indicate the best analytical method to be used.

The difficulty of matching the size of the analytical effort to efficiently provide the required visibility of risk, can be solved in successive steps. If sufficient time is allowed the analyst, a preliminary analysis may be conducted to predict the best analytical method to use for the formal analysis to follow.

The preliminary analysis to be performed should at least consider:

- (1) The contractual or binding system safety requirements. How accurately must safety be measured? A high degree of accuracy implies a detailed, quantitative analysis. Minimum allowable accident probabilities may be explicit in the contract.
- (2) How hazardous does the system seem? Does the system require a large or close man-machine interface? Are high energies stored in the system? Are weight or structural criteria such that normal safety factors must be reduced? Is the system operated in environments for which it was not designed? Are subsystems required to protect man and machine from severe environments? Affirmative answers imply highly hazardous systems.
- (3) What level of technology is required to design and build the system relative to the state-of-the-art? New ideas and ways of solving system design problems frequently imply an unusual element of risk.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 (Continued)

- (4) What level of technological skill is required to operate the completed system relative to estimated present skill levels of the user? A new type of system which requires the user to learn new skills, beyond merely acquiring systems familiarization, implies that he will also need to be aware of the new risks inherent in the system in more detail than users who have already mastered the required skills.
- (5) If the user is now operating, or is about to operate, a finished system, he may specify safety analyses which he already knows he needs. The specific problems he poses may dictate the method of analysis to be conducted, either directly or by inference. If not, compare his stated safety problems with 1 through 4 above.

The type and character of the safety problems should be formulated and the best method selected which will provide the required outputs, and will scope the system level for which the safety problem is formulated.

Finally an assessment of the available data must be made to determine the possibility of providing the required analytical outputs with the method selected (see Section 3). After screening the methods in such a manner, several methods may still appear to be practical. The analysis method requiring the least overall effort is normally chosen in that case. However, if the analysis of the immediate safety problems will point out additional areas where analysis will be required, then consideration must be given to using the method which provides a baseline for further analytical work. This may cause the analyst to recommend a method which involves a more extensive original analytical effort than would otherwise be chosen, so that material savings will be realized in future safety analyses.

An example of method selection drawn from actual experience on the Apollo Program is provided below:

The combined System Safety organization of NASA, Boeing TIE, and Bellcom conducted meetings to compile a list of possible potential accidents in the Apollo program. The accidents were prioritized on the basis of program experience, mission criticality and expectations of the likelihood of occurrence. The top priority safety problems centered around the Astronauts who were to fly each manned mission. The analytical problem was initially defined in qualitative terms and, in essence, said - "Identify all hazards which may cause death or injury of the Flight Crew from the time of entry into the launch pad at Kennedy Space Center through all following mission phases including splashdown and recovery from the Command Module of the spacecraft."

2.0

(Continued)

Several methods of analysis could provide hazard identification, but fewer methods could provide the relative criticalities of the risks incurred by the Flight Crew as they came within the area of influence of each hazard. Some means was required to identify those hazards for which the present risks were acceptable. The ideal method would provide numerical probabilities of each hazard causing the accident to be avoided, namely death or injury to one or more Astronauts. Fault Tree (logic diagram) and Failure Mode, Effects, and Criticality Analysis (FMECA) became the candidate methods.

A review of the available data disclosed that failure data would be very difficult to obtain in the form needed, and that in some cases the data sample was very small. This is characteristic of a system for which a low production quantity is required, such as a research program like Apollo. This forced the reliance on relative assessments of criticalities for each hazard identified. The lack of exacting failure data indicated that a better perspective of the problem could be maintained with the Fault Tree method rather than the FMECA method. The availability of some failure history, equipment level FMEA's and other types of engineering analyses was considered to fit into the Fault Tree method better than FMECA. Further, the analysis team was spread from East Coast to West Coast and team membership involved several agencies. The Fault Tree method provided an efficient communication and analysis management tool. The final considerations were analytical resources and the long term System Safety analysis requirements.

The potential accident of death to the Astronauts only began the list of many potential accidents which the user, NASA, wished to prevent. The utility of the Fault Tree in a complex study area, its capability to keep pace with the changeability encountered at this program level and the detail analysis documentation it provides, form an excellent baseline for future analysis. This baseline allows maximum conservation of analytical effort, and thereby minimizes long term manpower requirements. Had the study area been confined to a less complex system, say the Saturn Booster, then the FMECA approach may have been selected, particularly when consideration had been given to the analyses already in progress for that level of system study and the time available to complete the system safety analysis.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.1 METHOD SELECTION MATRIX

System safety studies must provide management visibility and engineering counsel regarding the safe construction and operation of systems. To accomplish this purpose there are several types of analysis results, or outputs, which may be reported singly, or in combinations which are most productive in terms of safety assurance in a given situation. These are listed as output requirements on the matrix on page 2-6.

The method of analysis should be effective for the study area under consideration from the viewpoint of time, cost, and method capability. The study areas are listed across the top of the method selection matrix.

The analysis methods are shown at the intersecting columns and rows for study areas and output requirements. These are suggested only as a guide, and use of the matrix should not replace an assessment of each specific situation.

USE FOR TYPEWRITTEN MATERIAL ONLY

STUDY AREAS

OUTPUT REQUIREMENT	PROGRAM ALL CENTERS	CENTER ALL PROGRAMS AT ONE CENTER	ALL PROGRAMS AT ONE CENTER	ALL GROUND SUPPORT SYSTEMS AND FLIGHT SYSTEMS	A GROUND SUPPORT SYSTEM OR A FLIGHT SYSTEM	GROUND SUPPORT SUBSYSTEM OR FLIGHT SUBSYSTEM	MODULE	COMPONENT
IDENTIFICATION OF POTENTIAL ACCIDENTS	GHA	GHA	GHA	GHA	GHA	GHA	FMECA	FMECA
	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	-
IDENTIFICATION OF HAZARDS	GHA	GHA	FTA	FTA	FTA	FTA	FTA	FMECA
	FTA	FTA	GHA	GHA	FMECA	FMECA & FRA	FMECA & FRA	FRA
IDENTIFICATION OF UNPLANNED AND PLANNED EVENT COMBINATIONS WHICH CAN CAUSE AN ACCIDENT	FTA	FTA	FTA	FTA	FTA	FTA	FTA	FMECA
	OSA-II	OSA-II	OSA-II	OSA-II	FMECA	FMECA	FMECA	-
IDENTIFICATION OF CHAIN OF PLANNED EVENTS WHICH INCREASE THE RISKS TO PEOPLE AND HARDWARE SYSTEMS	OSA-II	OSA-II	OSA-II	OSA-II	OSA-II	OSA-II	OSA-II	OSA-I
	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	-	-
ASSESSMENT OF DAMAGE EXTENT OR NUMBER OF PEOPLE WHO MAY BE AFFECTED WITHIN THE ACCIDENT INDUCED ENVIRONMENT	OSA-II	OSA-II	OSA-II	OSA-II	OSA-I	OSA-I	OSA-I	OSA-I
	FTA	FTA	FTA	FTA	GHA	GHA	-	-
PROBABILITY OF OCCURRENCE OF IDENTIFIED POTENTIAL ACCIDENTS	FTA	FTA	FTA	FTA	FTA	FTA	FTA	FMECA
	FMECA	FMECA	FMECA	FMECA	FMECA	FMECA	FMECA	FRA
SAFETY CRITICAL PARTS LISTS	FTA	FTA	FTA	FTA	FTA	FTA	FMECA	FMECA
	FMECA	FMECA	FMECA	FMECA	FMECA	FMECA	-	-
SAFETY OPERATING CRITERIA, STANDARDS, AND PROCEDURES	OSA-I*	OSA-II	OSA-II	OSA-II	OSA-II	OSA-I	OSA-I	OSA-I
	OSA-I	OSA-I	OSA-I	OSA-I	OSA-I	OSA-II	-	-

LEGEND Assume the analyst has been given the study area (column headings) and has been given, or has concluded, the type of output required (row titles at left). At the intersection of each column and row, the first and second choice of method is tabulated. Provided that the information needed for the method shown exists (see Section 3.0), it will be practical to attempt an analysis based on that method.

Abbreviations are as listed below for each method

GHA: Gross Hazards Analysis (See Section 4.1)
OSA-I: Operations and Test Safety Analysis (See Section 4.2)

OSA-II: Operations Safety Research (See Section 4.2)

FTA: Fault Tree Analysis (See Section 4.3)

*FRA: Fracture Mechanics Assessment (See Section 4.4)

FMECA: Failure Mode, Effects, and Criticality Analysis (See Section 4.5)

Block Key
to choices
1st
2nd

*Fracture Mechanics Assessment is a systems approach to module or component safety problems. In this sense FRA is used in the handbook because of the need to propagate this particular analysis method and because it is very exemplary of similar methods for other types of hardware, such as stress analysis on electrical/electronic equipment, break circuit analysis, and recent efforts to analyze explosion phenomena.

FIGURE 2-1

USE FOR TYPEWRITTEN MATERIAL ONLY

SECTION III

DATA INPUTS

3.0 DATA INPUTS

3.1 TYPES OF DATA

The system safety analyst will find that data required to conduct an analysis of a system are large in quantity and vary considerably. The quantity of data required depends on the size and complexity of the system to be assessed. However, the types of data that must be collected for the analysis are predictable. These types are discussed in the following paragraphs.

3.1.1 System Function and Description

In the conceptual phase system specifications should be gathered before the analysis begins. Procurement of the system is controlled by requirement specifications that define the user's objectives, design constraints, and requirements such as conformance to standards or codes.

In the developmental phase system design drawings must be gathered as the analysis begins. The most useful of these are system functional logic diagrams or flow diagrams. In all analyses, great use is made of system schematics; and in some analyses, module, drawer and component level schematics are necessary. Installation drawings are useful when assessing the possible effects of high energy release accidents such as high voltage shorts, explosions, and fires. Installation drawings help in the analyses of accident control equipment (inerting or water systems) and in assessing emergency egress capabilities. Detail part drawings are usually not useful except when safety critical components have been identified in the analysis. Analyses which are conducted after the system is built may be expedited by reference to technical manuals and operation and maintenance manuals.

3.1.2 System Environment

The system's environment may be determined from requirements specifications and design constraints. Further environmental data may be required as the analysis develops, to answer specific questions about the effects of environment on particular portions of the system. The environment may not be constant in time or may vary from one part of the system to another at any given point in time. It will be necessary to collect interface data which affects the system's function relative to safe use. Installation drawings are useful if spatial relationships are pertinent to failure mode causes or effects. The energy sources in the system being analyzed may not appear to be hazardous until the other systems in the accident induced environment are known.

USE FOR TYPEWRITTEN MATERIAL ONLY

3.1.3 Failure Data

Whether the analysis is going to be quantitatively evaluated or not, some failure data becomes necessary as it develops. Without any insight about relative failure probabilities, all failures may be considered equally likely. This will cause single failure points which are critical to safety to appear to be the most likely to cause an accident. Strangely enough, this may not identify the most critical failure potentials. Since the probability that a given fault will occur when it can cause the potential accident depends on both the failure rate and the total time it may be causative, multiple failures may be more likely to create the accident than one failure. Therefore, the probable time from the actual fault to the detection of that fault is required. If there is no means of "safing" the system upon detection of a critical fault, the time from detection to repair can be used. In the case of faults which will not be detected when they occur the best estimate to use is the time to periodic maintenance or the test frequency.

Any data which helps the analyst select critical failures is considered as "failure" data. A consideration of the safety factor in the design is helpful. If components are operated at or near their failure limits, the probability of failure is greater than if a large safety margin has been allowed. If the failure limits are not well defined for a component because of state-of-the-art limitations, then the chance for a design error in establishing safety factors is greater than when failure limits can be accurately estimated and proven in test programs. Usually when safety factors cannot be well established for the design, high factors are used. This in itself can sometimes pose a concern for the analyst.

If FMEA's have been conducted for components, modules, etc., of the system, these can be used to indicate the failure probability. FMEA's with quantitative evaluation are best, but caution is advised because the failure modes considered may not exactly coincide with the failure mode required in the safety analysis. See Paragraph 4.5 on use of FMEA's as an analytical tool.

Direct, raw failure history obtained during test and operation of the system is useful if found in sufficient quantity. Since direct history on the components is usually not sufficient in itself, this may be complemented by generic failure data from PRINCE, FARADA,* or other reliability failure data files. These generic rates are hard to use for two reasons. First, the stated failure rates include all known modes of failure for that component. In some cases both primary and secondary failures have been grouped together, and in others only primary failures have been reported. The analysis normally requires failure rate for only a few of all possible modes, both primary and secondary. Secondly, the conditions under which the failures actually occurred may be significantly different than the operating conditions experienced by the

* See Paragraph 3.1.6.2 a and b

3.1.3 (Continued)

component in the system under study. This leads to "fudge factors" which are a large source of error in the final probability of failure of the component in question. The selection of the most accurate failure rate is therefore quite difficult and time consuming.

3.1.4 System Simulation Data

Employment of system simulation testing and data may provide an excellent basis for safety judgments and design decisions on new systems. A reasonable approximation of the use environment can be obtained by testing portions of the system which are deemed to be essentially independent or whose interaction with the rest of the system can be simulated. Additionally, some cause-effect characteristics may be developed mathematically upon a physical basis. This can be done with reasonable accuracy for electrical networks and structural components because of the accurate specification of manufacturing tolerances and the ability to express theoretical relationships.

3.1.5 Other Studies

When engineering studies of subsystems are found, they may be useful in avoiding a new analysis of the same subsystem. The analysis is more useful if a quantitative evaluation is provided for the probability of the failure or fault event of the subsystem.

3.1.6 Sources of Data

Much of the data to be collected is found in engineering libraries, drawing files, and general libraries and information centers maintained by both private and government agencies. The systems analyst will find, however, that most of the information procured from data centers must be complemented by information gained through direct interface with the organizations who create the data. Well established communications with these organizations will facilitate both the understanding of the data collected, and will ensure that a knowing and realistic use is made of the information obtained. Misused data causes the creation of an un-used analysis. The most important quality of an analysis is validity.

3.1.6.1 Data Generating Organizations

a. Design Engineering

Design Engineering is a source of valuable information on the operating and functional characteristics of the system. Knowledge of proposed changes to the system can be acquired during the conceptual and initial design change stage, and suggestions

3.1.6.1 a. (Continued)

made to the designers to provide a safer, cost-effective change. System design changes which are needed for improved system safety can be discussed with the designers to select the most effective design alternative with respect to safety and system effectiveness.

The interface between system safety analysts and Design Engineering requires a "day-to-day" working relationship between members of each organization. The results of this close relationship are inherently beneficial to both organizations.

b. Maintainability

Maintainability is a design discipline that provides for ease, economy and safety in all maintenance functions and the use of maintenance equipment. Therefore, system safety engineers work with Maintainability to perform safety analyses on maintenance equipment and to certify the safety of maintenance equipment design and maintenance operations.

c. Human Engineering

Human engineering and system safety engineers must use human factor statistics as a part of the safety analyses. A study of man-machine relationships complements system safety by providing additional emphasis on human error analysis and error reduction. These are critical considerations in determining potential system modes that can result in hazardous conditions. Identification and analysis of the overall hazardous consequences of a given failure event require an understanding of human capabilities and limitations as well as the interfaces between subsystems, systems, and environments. Man-machine relationships to be effective must be integrated with system safety to provide a logical and consistent continuum throughout the life span of the aerospace system.

d. Reliability

A function of Reliability is system hardware analysis for failure data; such as failure modes, failure effects, mean time between failures, probabilities of failure and assessment of system failures on mission accomplishment. Much of this type of data is used for both qualitative and quantitative system safety analysis. For example, existing and substantiated failure modes and effects data is an invaluable aid in the qualitative logic diagram analysis of a system. In a quantitative logic diagram evaluation, hardware failure rate data is a necessary item. Conversely, the results of a system safety analysis may have a direct impact upon reliability; such as requiring further testing of certain hardware or improving the reliability of a particular system element, to decrease the likelihood of system

USE FOR TYPEWRITTEN MATERIAL ONLY

3.1.6.1 d. (Continued)

damage or human injury. It should be noted that complete numerical parity should not be expected because reliability "numbers" normally refer to both primary and secondary failures for particular failure modes. Thus, it is entirely possible for a system to have reliability which is the complement of one failure per 1000 operating hours and a probability of an injurious or damaging undesired event of one per 1,000,000 operating hours.

e. Health and Safety

System Safety is concerned with test, assembly, checkout, maintenance and use of systems which provide a possibility of serious injury, loss of life, loss of equipment or significant equipment damage as a result of the existence of the system. Health and Safety is concerned with providing a safe working environment for employees. There is some overlap between the two functions and in this case the more stringent standards of acceptability would apply.

The Health and Safety activity can aid system safety engineers by providing information and data on human factors, toxic materials, anthropometric considerations and other specialized data related to the human working environment.

f. Quality Assurance

The system significance of a particular event or part detail cannot be determined by study of the design alone. Therefore, predictive system safety analyses must be made from drawings, procedures and other documented instructions. The accuracy of each analyses and the conclusions derived from them are dependent on activities of quality technicians and inspectors in assuring that instructions are followed.

Quality requirements are determined and satisfied throughout all phases of contract performance. The Quality Assurance program ensures that quality aspects are fully included in all designs and that high quality is obtained in the fabricated articles. Any change required to improve components, subsystem, or system performance without compromising quality, reliability or safety should be incorporated at the earliest practical point in development and fabrication. The Quality Assurance program provides for the early and prompt detection of actual or potential deficiencies, system incompatibility, marginal quality, and trends or conditions which could result in unsatisfactory quality. Objective evidence of quality conformance, including records of inspection and test results is useful data for system safety analyses to provide a high level of confidence in the representation of potential system faults and confidence in the assignment of probabilities to the fault events.

USE FOR TYPEWRITTEN MATERIAL ONLY

3.1.6.1 (Continued)

g. Test Planning and Reporting

Special tests are conducted on hardware end items for reliability data, qualification, quality assurance, and system hardware integration. From these tests considerable data is produced which is useful for system safety evaluation. Conversely, requirements for special tests to obtain data specifically needed to assure system safety may result from system safety analyses.

System Safety analyses conducted on proposed test plans may initiate special test procedures and corrective measures to existing test plans.

h. Configuration Management

Configuration Management describes, identifies, and controls system configuration throughout the definition, development, production and change phases. System safety analyses require a well defined baseline configuration so that changes in configuration may be assessed after the basic system analysis is completed. Establishing the baseline configuration engineering data is a function of Configuration Management.

3.1.6.2 Data Storing Organizations

Specific organizational sources of data for the conduct of system safety analyses are listed in AFSC Design Handbook, DH 1-6, Chapter 2. Brief descriptions of four large data storage and retrieval organizations are included here to typify what is available to systems analysts.

a. Parts Reliability Information Center

The NASA Parts Reliability Information Center (PRINCE) is a specialized data center developed and maintained by the George C. Marshall Space Flight Center. The PRINCE provides an automated data storage and retrieval system containing technical information which is useful to reliability analysts. The data contained can also be used by system safety analysts in compiling specialized failure history for analysis evaluations.

b. Failure Rate Data Handbook

The FARADA Program document is a component part "Failure Rate Data Handbook" (FARADA). Updating and expansion of the data is accomplished by the FARADA Information Center at the U. S. Naval Ordnance Laboratory, Corona, California.

3.1.6.2 (Continued)

The Handbook contains component and part information relative to failure rates generated by contractors and agencies engaged in design, development and production of military and space program equipment. The failure rates contained in the Handbook are obtained from specific engineering data and test results.

c. Defense Documentation Center

The Defense Documentation Center (formerly ASTIA) is a large storage and indexing program of all types of scientific and technical information from many sources including federal agencies, industrial concerns, educational institutions, and research foundations. Information on hardware, software and complete systems is available, and many references and papers on analytical procedures and methods are easily found in the Center.

d. Interservice Data Exchange Program

The Interservice Data Exchange Program (IDEP) is a data storage and filing program which can be used by the analyst to acquire information for system safety assessment at all levels of complexity from components to complete programs or projects. The objectives of the IDEP program are:

1. To avoid repetition of tests already satisfactorily accomplished.
2. To provide prompt indication of possible failure modes.
3. To reduce duplicate expenditures for developmental parts testing and non-standard parts justification.
4. To encourage standardization of methods of test and test reporting.
5. To facilitate direct inter-contractor technical contacts on related problems on a timely basis.

USE FOR TYPEWRITTEN MATERIAL ONLY

INPUT DATA		METHOD	GROSS HAZARD ANALYSIS	OPS SAFETY ANALYSIS	FAULT TREE	FRACTURE MECHANICS ASSESSMENT	FMECA
		REQUIREMENT SPECIFICATIONS	*	▼	*	*	*
		SYSTEM SPECIFICATIONS	*	▼	▼	*	*
		DETAIL SPECIFICATIONS	*		*	▼	▼
		FLOW DIAGRAMS	▼	*	▼	*	▼
		SCHEMATICS	*		▼	*	▼
		INSTALLATION DRAWINGS	*		*	*	*
		DETAIL DRAWINGS	*		*	▼	*
		O&M MANUALS	*	*	*	*	*
		TEST & CHECKOUT PROCEDURES	*	▼	*	*	*
		OPERATING PROCEDURES	*	▼	*	*	*
		TEST REQUIREMENTS	*	▼	*	*	*
		STANDARDS	*	*	*		*
		WAIVERS & DEVIATIONS		*	*		*
		FAILURE REPORTS		*	▼	*	▼
		FMEAS			*		
		OPERATIONS ANALYSIS	*	* Other Safety	*		*
		MAINTAINABILITY ANALYSIS		*	*		*
		CRITICAL PARTS LIST			*		
		SAFETY PROCEDURES AND REGULATIONS	*	▼	▼	*	*
		FRACTURE MECHANICS ASSESSMENT			*	*	*
		GROSS HAZARD ANALYSIS		*	*	*	
		FAULT TREE ANALYSIS					*
		MAN-MACHINE INTERFACE ANALYSIS	*	*	*		
		OTHER SYSTEMS ENGINEERING ANALYSIS	*	*	*	*	*

LEGEND

- * SIGNIFIES DATA WHICH IS USEFUL FOR THE METHOD AT THE LEFT**
- ▼ SIGNIFIES DATA WHICH IS MANDATORY FOR THE SUCCESSFUL COMPLETION OF THE METHOD ON THE LEFT.**

FIGURE 3-1

SECTION IV
ANALYTICAL METHODS

USE FOR TYPEWRITTEN MATERIAL ONLY

4.0

ANALYTICAL METHODS

This section describes various qualitative and quantitative techniques which may be used in safety analysis. A brief discussion of data sources available to the safety analyst, and methods to resolve identified hazards are included.

The complexity of present and proposed aerospace systems, the number of individuals and organizations involved in their development, and the inherent desire for multi-mission capability all tend to create system safety problems. Increasing system acquisition and modification costs require that a system safety approach be identified early in the development stage so that it may have some impact upon design requirements and trade-off decisions. The degree of safety achieved in an aerospace system is a basic design problem; its resolution lies in the application of safety engineering and its assessment is gained through engineering analysis.

Analyzing system and subsystem design is the fundamental act by which insight into safety design effectiveness can be accomplished. Without safety analysis, safety design defects are exposed by the unpleasant experience of accident investigation.

The various safety analysis techniques to be discussed in this handbook are Gross Hazards Analysis, (4.1); Operations and Test Safety Analysis and Operations Safety Research, (4.2); Fault Tree or Logic Diagram Analysis, (4.3); Fracture Mechanics Assessment, (4.4); and Failure Modes, Effects and Criticality Analysis, (4.5).

Cautions in Safety Analysis

Although various safety analysis techniques may be available, these should not be regarded as tools to be applied to every design problem, particularly those where a definite alternative is clearly the proper solution. Statistical and analytical techniques are not a replacement for common sense. This is particularly true in analyzing research and development programs. Employment of a mathematical technique may indicate that the probability of an undesirable event occurring due to a given set of circumstances is 1×10^{-6} . If the event would cause loss of the system and can be precluded without significant cost or degradation of performance, why accept any risk? The concept of establishing an acceptable level of risk can result in acceptance of unnecessary risk. The purpose of safety analysis is to expose hazards and minimize or preclude risk. Predictions may be inaccurate by a magnitude when an event is associated with human behavioral variances.

4.1 GROSS HAZARDS ANALYSIS (See Appendix A)

4.1.1 Summary Description of Technique

The technique of gross hazards analysis is a comprehensive, qualitative hazard assessment applicable to complete systems or major segments of a system. The gross hazard study should be conducted early in the design phase or modification phase of the system.

A good gross hazards study will identify critical areas of the system, product, or end item which should be subjected to additional safety analysis or which indicate a need to change a design requirement. The study will also provide management personnel with visibility of the adequacy of safety features of the system and information about the likely contingency conditions. The study should help to identify routine or special test requirements and will be very valuable in establishing priorities to allow scheduling and manning of the safety effort. A necessary result of the gross hazard study will be the establishment of upper and lower limit definitions for standard hazard categories in terms of the system under study. Controlling design criteria such as, existing codes, regulations, standards or policies and procedures may be identified to assure coverage of all gross hazards identified in the study. Any gross hazards which have been identified, and for which no controlling design criteria exist, should be covered by specific criteria in the gross hazards study.

4.1.2 Applications of Gross Hazards Analysis

4.1.2.1 Priorities and Ground Rules

The gross hazards study will allow the definition of the system safety task. With this task defined for the system under study it will be possible to establish system safety goals and priorities in accordance with established mission or contract objectives. The analysis schedule and manpower requirements may then be planned through the program phases which have been forecast.

Standard hazard categories spelled out in terms of the system under study should be clearly defined. The upper and lower limits of each hazard category should be clearly defined because these will establish the ground rules for setting goals and priorities.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.1.2.2 Design Control Criteria

Criteria to be applied to the system during design activity to minimize hazards to personnel or equipment should be identified for the designers. This criteria will include existing safety codes, regulations and standards as well as design standards, codes, and procedures applicable to the system, subsystems and components under study. Where existing criteria are inadequate for the level of safety desired, planning to correct the inadequacies should be initiated. The types of follow-on safety analysis required to continue the system safety analysis should be specified in accordance with the advantages, including cost effectiveness of each type of analysis.

4.1.2.3 Implementation

Action items which result from gross hazard studies should be specifically assigned to assure completion. Assignments for specific phases of the analysis which may be performed by designers and personnel other than the system safety analysts should be planned and prioritized to the level of detail necessary to assure successful completion of the study.

4.1.3 Input Data Required for Gross Hazards Analysis

The gross hazards analyst must be supplied with the system specifications, diagrams, manuals, procedures, requirements and history for use in familiarization, evaluation, and planning corrective action. Hazard and failure experience of similar, related or interfacing systems should also be obtained. (See Figure 3-1).

4.1.4 Gross Hazards Analysis Procedure

The basic gross hazards analysis procedure consists of breaking the system down into units of various types, by use of functional flow diagrams or other techniques, and then subjecting each unit to analysis for gross hazards.

All systems have a purpose. To achieve this purpose, operation or functioning of the system can be broken down into a series of steps or functions. These steps or functions are inter-related in such a way as to perform the purpose of the system. The functions or steps, and their relationships, can be shown in a form commonly known as a "flow diagram". Flow diagrams can be prepared to show as much detailed information as is desired. The amount of detail required in flow diagrams prepared for a given system is a function of the depth of analysis required. Common practice is to begin with a gross functional flow diagram and prepare succeeding more detailed diagrams until the desired level of detail is achieved.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.1.4 (Continued)

Some flow diagrams may have already been prepared on a system as an aid to basic system design. However, if the analysis must be conducted on a system which is still in a preliminary design stage, few flow diagrams will have been prepared. Preparation of necessary system flow diagrams must, therefore, be accomplished through the safety analysis function. The process of preparing these flow diagrams can provide system understanding, more detailed identification of system hazard areas, a basis of communication with other engineering functions, and generates information for more detailed safety analysis.

When a gross hazardous condition is identified, the system event, subsystem, operation or facility is listed as a safety critical item. The listing should include a specific description of the hazard.

Each identified gross hazard should then be eliminated, circumvented or controlled by a recommendation from the system safety organization for an engineering change to the design, or a procedural change, or both.

If the fault which leads to the gross hazard cannot be readily determined, a recommendation for more detailed safety analysis should be made.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.2 OPERATIONS SAFETY ANALYSIS (See Appendix B)

4.2.1 Summary Description of Technique

The technique of Operations Safety Analysis is a means of identifying tasks that are hazardous in the operation of a system. There are two major areas of consideration. In this handbook they are divided into Operations and Test Safety Analysis and Operations Safety Research.

4.2.2 Application of Operations Safety Analysis

The results of OSA's, specifically safety requirements for each task, can be used as either direct input to the detailed procedures for the task, or can provide a baseline for criteria standards, manuals, or handbooks against which the detailed procedure is written.

4.2.3 Input Data Required For Operations Safety Analysis

The operational safety analyst will require as basic data the project requirement specifications, the system specifications, the operating procedures and the appropriate safety procedures and regulations that have been established for the type of operation being analyzed. In addition, test requirements and test and checkout procedures are needed for OSA-I. Many other types of data can be useful as indicated in Figure 3-1.

4.2.4 Operations Safety Analysis Procedure

Since each of the major areas of consideration are unique, the analysis procedures are described separately.

4.2.4.1 Operations and Test Safety Analysis (OSA-I)

The Operations and Test Safety Analysis (OSA-I) method identifies operations that are inherently hazardous or, which by the nature of the function sequences, can lead to development of hazards in the operation of a system. This method can be used in all aspects of system operation from construction to mission termination.

The objective of performing OSA's is to ensure that hazards, existing or developing during a particular task, are identified, documented and brought to the attention of the proper authorities for resolution. Such hazards may result from the task itself, or from interaction of other work being done concurrently with the task. The OSA's will include corrective action recommendations which serve to eliminate these hazards, or reduce them to an acceptable level. Each task is reviewed and the reasoning for a particular safety requirement is recorded to substantiate program decisions.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.2.4.1 (Continued)

Each task (act, process, or test) can be analyzed individually to ensure complete investigation of all situations requiring safeguards, special equipment, or specific instructions (e.g., cautions, warnings, or verifications) to avoid personnel injury or significant equipment damage. Previous analyses of hazards in specific areas of operation should be used to the maximum extent.

4.2.4.2 Operations Safety Research (OSA-II)

As the name implies, operations safety research involves the safety research of operations. In this method, operations are researched to determine how to create and use systems in the safest manner. The techniques used in operations research provide a scientific approach to decision making that involves the operations of a system. The relative safety of alternatives is a characteristic of the system similar to reliability, maintainability, cost effectiveness, flexibility, and operability. The use of operations research assumes that the system user's objectives include maximum safety within the constraints of minimum cost and other objectives of the mission.

The principal techniques of operations research which may be applied to optimizing system safety are Linear Programming, Network Analysis, Dynamic Programming, Game Theory, Queing Theory, Markov Chains, and the techniques of Simulation. All systems engineering analysis methods use these techniques to some degree, because of the fundamental nature of the problem of systems analysis and design. This problem is concerned with achieving a balance of many conflicting parameters and variables to accomplish the objectives of the system user. A brief explanation of the Linear Programming method and Network Analysis are provided in Appendix B, Part II.

4.2.4.3 Human Error Prediction Techniques

In both of the above Operations Safety Analyses, a consideration of possible human error may be appropriate.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3 FAULT TREE ANALYSIS (See Appendix C)

4.3.1 Summary Description of Technique

The System Safety fault tree logic diagram analysis method consists of three basic analytical elements; viz: -

1. System Safety fault tree development
2. " " failure data development
3. " " fault tree evaluation.

The System Safety fault tree is a logic oriented graphic representation of independent failure combinations which may interact or may singly produce system failures or undesired events within normal system operating modes. The diagram alone is a qualitative tool. When combined with failure data inputs, an evaluation can be made and dominant paths can be identified. The analysis then becomes an effective quantitative approach to accident prevention.

The following steps are essential as a basis for a systems approach to safety and will enable identification of undesired (hazardous) events which are to be maintained at an acceptable level:

1. Identification of undesired events;
2. Structuring of undesired events into a logic diagram;
3. Determination of fault inter-relationships;
4. Evaluation for "likelihood" of undesired events; and
5. Trade-off decisions and/or corrections.

Steps one and two are necessary to develop a "Top" logic diagram which serves as a guide showing how and where the tree is to be developed (or expanded) by further analysis activity. The "Top" logic diagram organizes all of the logic relationships unique to a system into a pattern which provides an orderly and logical manner for analyzing the system hardware and software functions.

The variable logic relationships which are unique to a system and must be structured are such things as: (1) operating modes, (2) mission phases and/or operations, (3) degree of man/machine relationship in the system (4) inter-relationships of the Centers with the system functions, and (5) functional order of the system.

Step three is the development of the fault tree analysis which starts with the "Top" logic diagram structure and proceeds through hardware level.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3.1 (Continued)

Step four is an evaluation of the completed logic diagram for
(a) determining the likelihood of undesired events, and
(b) determining the identity and ranking of series of events
and event relationships leading to the undesired event (s).

Step five is a further assessment of the analysis results to determine what corrective action is required. Proposed corrections such as design changes, procedure changes, training methods, added safety features, etc., can be evaluated in the context of the fault tree for the desired improvement.

Two points are vital to a meaningful and useful analysis. First, the output of an analysis is only as valuable and reliable as the effort and information applied to the analysis. Second, configuration control of the hardware and the operating procedures must be maintained lest erroneous conclusions be drawn from the analysis.

System Safety fault tree analysis is dependent and complementary to many other engineering functions. These include:

1. Configuration management for a baseline configuration, changes, specifications, requirements, verification and certification of manufactured end items, data on operating time or cycles, and schedules on approved changes.
2. Design engineering for information on the operating and functional characteristics of the system and the proposed changes.
3. Quality assurance for providing a level of confidence that the equipment and system conform to the documentation.
4. Test and operations for plans and data which may be used in the fault tree evaluation.
5. Reliability for such failure data as failure modes, effects and criticality analyses, failure rates, mean-time-between-failures, failure probabilities, and assessment of system failures on mission accomplishment.
6. Maintainability for maintenance functions and use of maintenance equipment.
7. Human engineering for equipment design characteristics providing efficient, accurate and safe utilization of the equipment by the operators.
8. Health and safety for provisions of a safe working environment for employees.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3.1 (Continued)

While it is recognized that there is a significant degree of inherent compatibility between System Safety analyses and reliability, complete numerical parity should not be expected. Reliability figures refer to both primary and secondary failures for particular failure modes.

A system may have a reliability which is the complement of one failure per 1000 operating hours but the probability of a significant undesired event (accident) could be one per 1,000,000 operating hours. It is possible that safety considerations make it necessary to attain greater reliability from some equipment even though the system reliability is already adequate to perform the desired mission.

4.3.2 Applications of Fault Tree Analysis

The fault tree method is generally applicable at any level of complexity of system or any size of study area. The cost-effectiveness of the fault tree method remains approximately constant at all levels except when analyzing only detail parts, and no system analysis is required. Fault tree methods are especially well adapted to large program level analyses. When the method is applied in program wide study areas, exceptionally strong technical communications between the analysts involved must be established at the beginning and maintained throughout the analysis. The analysis of system operating modes and phases at the top of the tree progresses more slowly than analysis at the hardware level because of the many alternatives usually encountered. However, the fault tree development at the top levels, where many of the contingencies and operating alternatives are sorted out, can point out any large risks inherent in the system. For example, in the Apollo program, the sequence of missions and their associated objectives greatly affect the risks incurred by the astronauts. The top tree may point out these incurred risks, and a new sequence can be modeled to assess the trade off benefits.

4.3.3 Input Data Requirements For Fault Tree Analysis

After defining the scope of the system to be analyzed, certain information must be gathered so that the system may be characterized and pertinent aspects simulated for analysis. (See Fig. 3-1)

4.3.3.1 System Function and Description

System specifications should be gathered early. These will not only provide a description of the system, but will explain why certain design concepts are used when the analyst is studying system logic diagrams, flow diagrams and schematics. Detail part drawings are seldom useful, unless the analyst is totally unfamiliar with the components and modules in the system. Analyses conducted after a system is built can be expedited by reference to technical manuals and operation and maintenance manuals.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3.3.2 System Environment

The system's environment may be determined from requirements specifications and design constraints. Further environmental data may be required as the tree develops, to answer specific questions about the effects of environment on particular portions of the system. The environment may not be constant in time or may vary from one part of the system to another at any given point in time. It is sufficient in the beginning of the analysis to collect general environmental data, and gather detailed data only as required. Since other systems which interface with the system under analysis form part of the environment, it will be necessary to collect interface data which affects the system's function relative to safe use. Installation drawings are useful if spatial relationships are pertinent to failure mode causes or effects. The energy sources in the system being analyzed may not appear to be hazardous until the other systems in the accident induced environment are known.

This inter-system effect may cause some difficulty if the adjoining system is outside the scope of the authorized analysis. A judgment must be made about the extent of analysis required to complete the fault path in the other system to the potential accident. Since a finding such as this reverses the basic fault tree process, a new study should be recommended for potential accidents caused by the affected adjoining systems. If the top potential accident is defined in sufficiently narrow terms at the outset, this reversal may never occur. It is extremely difficult, however, to turn away from a legitimate safety concern because it falls outside the range of the original task. This facet of fault tree analysis, which seems to lead the analyst, is most beneficial because it points out problems which would not normally be detected. This aspect also poses a problem to the system safety manager, since he must guard against losing sight of the original problem.

4.3.3.3 Failure Data

Whether the tree is going to be quantitatively evaluated or not, some failure data becomes necessary as the tree develops. Without any insight about relative failure probabilities, all failures may be considered equally likely. This will cause single failure points and paths adjoining them through OR gates to the potential accident to be critical. Strangely enough, this may not identify the most critical paths. Since the probability that a given fault will occur when it can cause the potential accident depends on both the failure rate and the total time it may be causative, multiple (simultaneous, sequential, or random) failures may be more likely to create the accident than one failure. Therefore, the probable time from the actual fault event to the detection of that fault is required. If there is no means of "safing" the

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3.3.3 (continued)

system upon detection of a critical fault, the time from detection to repair can be used. Maintainability analysts should be able to provide accurate estimates of the required period of maintenance. In the case of faults which will not be detected when they occur the best estimate to use is the time to periodic maintenance or the test frequency. If safety is truly jeopardized in the case of undetected failures, increased test or maintenance frequency may be a sound solution. The addition of a monitoring device may be advisable, if it does not create an increase in the hazard level or increase the probability of the occurrence of the basic fault event.

Any data which helps the analyst select critical paths is considered as "failure" data. At one extreme, the analyst may have some expert provide a qualitative assessment, or he may have to rely on his own judgement on each component failure or basic fault event. A consideration of the safety factor in the design is helpful. If components are operated at or near their failure limits, the probability of failure is greater than if a large safety margin has been allowed. The possible effect of the man-machine interfaces from design through use should be "added" to this safety factor rule.

4.3.3.4 Other Studies

When engineering studies of subsystems are found, they may be useful in avoiding a second analysis of an undesired event in the same subsystem using the fault tree. An FMEA of the subsystem may include the failure modes needed. The FMEA is more useful if a quantitative evaluation is provided for the probability of the failure or fault event of the subsystem. See Section 4.5 on the use of FMEA's as an analytical tool. Engineering analyses other than FMEA can also be used to supplant further development of the tree for an undesired event. It is often helpful to informally extend the tree beyond the level that the engineering analysis is to be used when assessing the adequacy of the substitution. Three or four levels of tree usually are sufficient for this purpose.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.3.4 Fault Tree Procedure

The fault tree is a logic oriented graphic representation of parallel and series combinations of independent failures and operating modes that can result in a specified undesired event. The diagram can be quantified when required to provide a relative measure of the paths leading to the events.

The term "event" denotes a dynamic change of state that occurs to a system element, which may be hardware, software, personnel and/or the environment. If the event results in not achieving the intended function, or is achieving an unintended function, it is known as a fault event. Conversely, if an intended function is achieved as planned, it is known as a normal event.

Fault events may be basic events or gate events. Basic events are independent events whereby system elements (usually at component level) go from an unfailed state to a failed state and they are related to a specific failure rate and fault duration time. Basic events are used only as inputs to a logic gate.

A gate event is one which results from the output of a logic gate and is therefore a dependent event. As a fault tree progresses, gate events on one level become inputs to gate events on the next higher level.

In fault tree analysis the inherent modes of failure of system elements are referred to as primary events, secondary events and command events, and are depicted on the fault tree as the combination of basic events and gate events. Primary, secondary and command factors are defined as follows:

Primary Failure: Failure initiated by failures within, and of, the component under consideration, e.g., resulting from poor quality control during manufacture, etc., applied only to the component during Fault Tree Analysis when a generic failure rate is available.

Secondary Failure: Failure initiated by out of tolerance operational or environmental conditions, i.e., a component failure can be initiated by failure not originating within the component.

Command Failure:* The component was commanded/instructed to fail i.e., resulting from proper operation at the wrong time or place.

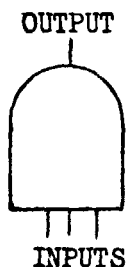
*Component may not always have command failure mode (e.g. a standard bolt) in which case this mode may be disregarded.


USE FOR TYPEWRITTEN MATERIAL ONLY

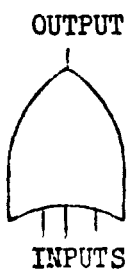
4.3.4 (Continued)


The development of a fault tree starts at the top or undesired event. The analysis determines what events can cause the undesired event. These become inputs to the top event. They can be two or more events, any one of which can cause the top event. Otherwise, they can be two or more events all of which must occur at the same time to cause the top event. The first group pass through an "OR" gate to get to the top event. The second group pass through an "AND" gate to get to the top event. The analyst then determines what can cause the input events. Each branch can be developed independently or concurrently. At some level below the top event the analyst will arrive at a piece of hardware (or subsystem). Each piece of hardware (or subsystem) can fail in three or less ways (i.e., primary failure, secondary failure, or commanded failure).

The dynamic change of state is defined as a binary type event, being either in the ON or OFF state. The ON state (or 1) corresponds to a failed condition and the OFF state (or 0) corresponds to an unfailed condition. By representing events and gates in a binary manner, logic diagrams can be analyzed by the techniques of Boolean algebra.

FAULT TREE SYMBOLS

AND GATE describes the logical operation whereby the coexistence of all input events is required to produce the output event. When hand sketches of fault trees are made a dot is placed in the center of the symbol to avoid confusion to the draftsman, thus .

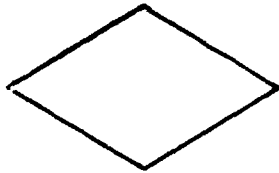


OR GATE defines the situation whereby the output event will exist if one or more of the input events exists. When hand sketches of fault trees are made a plus sign is placed in the center of the symbol to avoid confusion to the draftsman, thus .

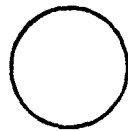


The rectangle identifies an event (gate event) that results from the combination of fault events through a logic gate. The words describing the event are placed within the box. When machine drafting with computer control is used, the computer program will limit the number of character spaces that can be used in any one block.

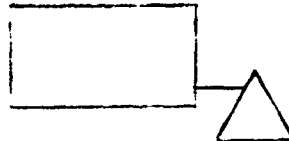
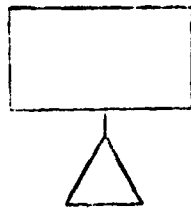
4.3.4 (Continued)



The diamond describes a fault event that is considered basic in a given fault tree. The possible causes of the event are not developed either because the event is of insufficient consequence or the necessary information for further development is unavailable. It also can indicate non-development because an analysis already exists that is of satisfactory depth and breadth. In any case the reason should be stated, either in the symbol box or in cross-referenced notes.

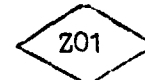


The circle describes a basic fault event that requires no further development. The frequency and mode of failure items so identified is derived from empirical data. The rate of occurrence of such a primary event is normally the generic failure rate of the component for the particular failure mode.



The transfer triangle indicates that a section of the fault tree is drawn once and used in more than one place on the tree. If the triangle is drawn under the event block, it means that the diagram that would appear underneath is drawn under some other

event box in the tree. Since all events and logic below the triangle are transferred from one event to another, all necessary and sufficient conditions to cause both events must be exactly similar. If the triangle is drawn at the side of the event block, it means that the diagram drawn below is used in its entirety to satisfy the input conditions for more than one event. The event designation within the box is identical on both diagrams. Cross reference between a transferred diagram and the events which use it is accomplished by coding the triangles with the same letters or numbers.



The numbers and letters appearing in the symbols above are coding devices to permit the diagrams to be drawn by a computer controlled drafting machine. They are also used to identify an event; for example, "the E-4 event on the IIT Diagram."

4.3.4 (Continued)

A Sample System

An automatic gas hot-water heater is a good example to use in illustrating the elements of a system. The task of the system is to provide hot water in our house at all times. In order to perform this task a system is used whose components consist of a water tank, a gas heater, a temperature measuring and comparing device to regulate the system, a controller (actuated by the temperature measuring device) to turn a valve to control the flow of the gas, a pressure relief valve (to permit excess pressure to escape if the heater fails to shut off), a cold water intake pipe, a hot water pipe leading to the faucets, and an exhaust pipe for the flue gases from the gas heater.

From the view of task performance, we can examine the system to see in what ways failure or malfunction of the components can stop delivery of hot water when we want it, or, more importantly, when the system might get out of control and the tank rupture or gas escape. The interrelations of the components are apparent to anyone familiar with the operation of such a heater and we can trace through the system the effects of any component breakdown.

In normal operation the tank is filled by cold water. The water temperature in the tank is monitored by the temperature measuring device and this temperature is compared with the preselected temperature. When the water temperature in the tank is less than the desired temperature, the controller opens the gas valve, allowing gas to flow to the burner. When the water in the tank reaches the desired temperature, the controller causes the gas valve to close, allowing no more gas to flow to the burner. The pressure relief valve acts as a safety device by venting excessive pressure.

EXAMPLE OF A SYSTEM

(DOMESTIC HOT WATER SYSTEM)

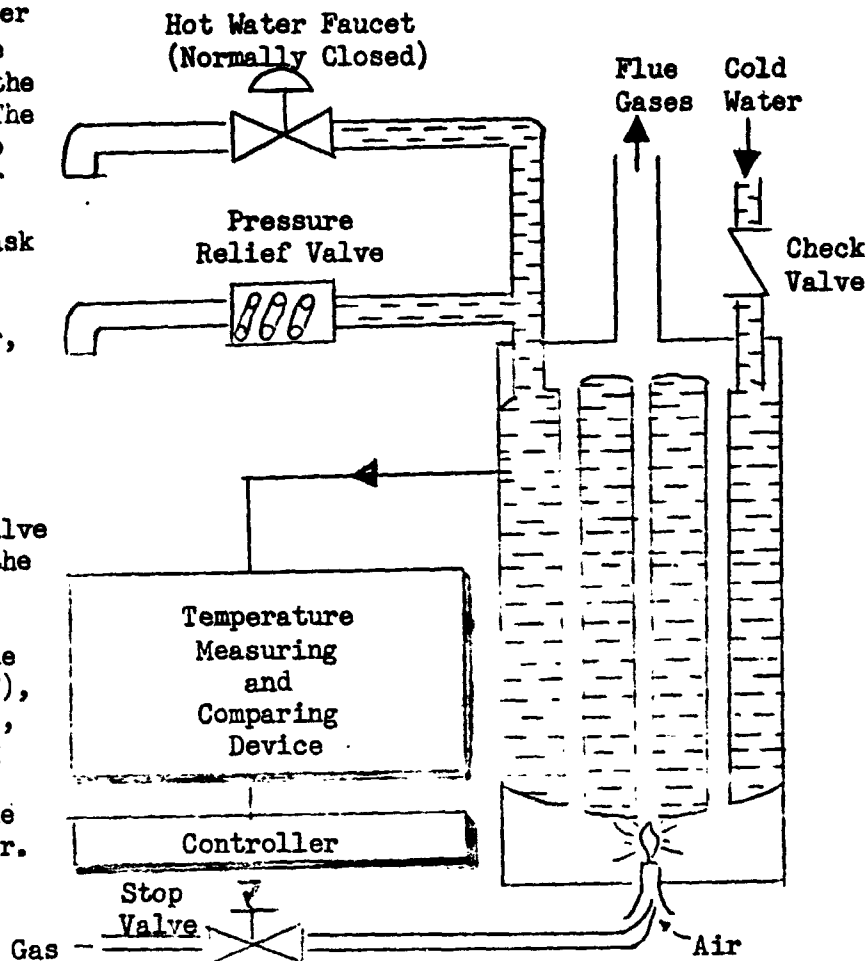
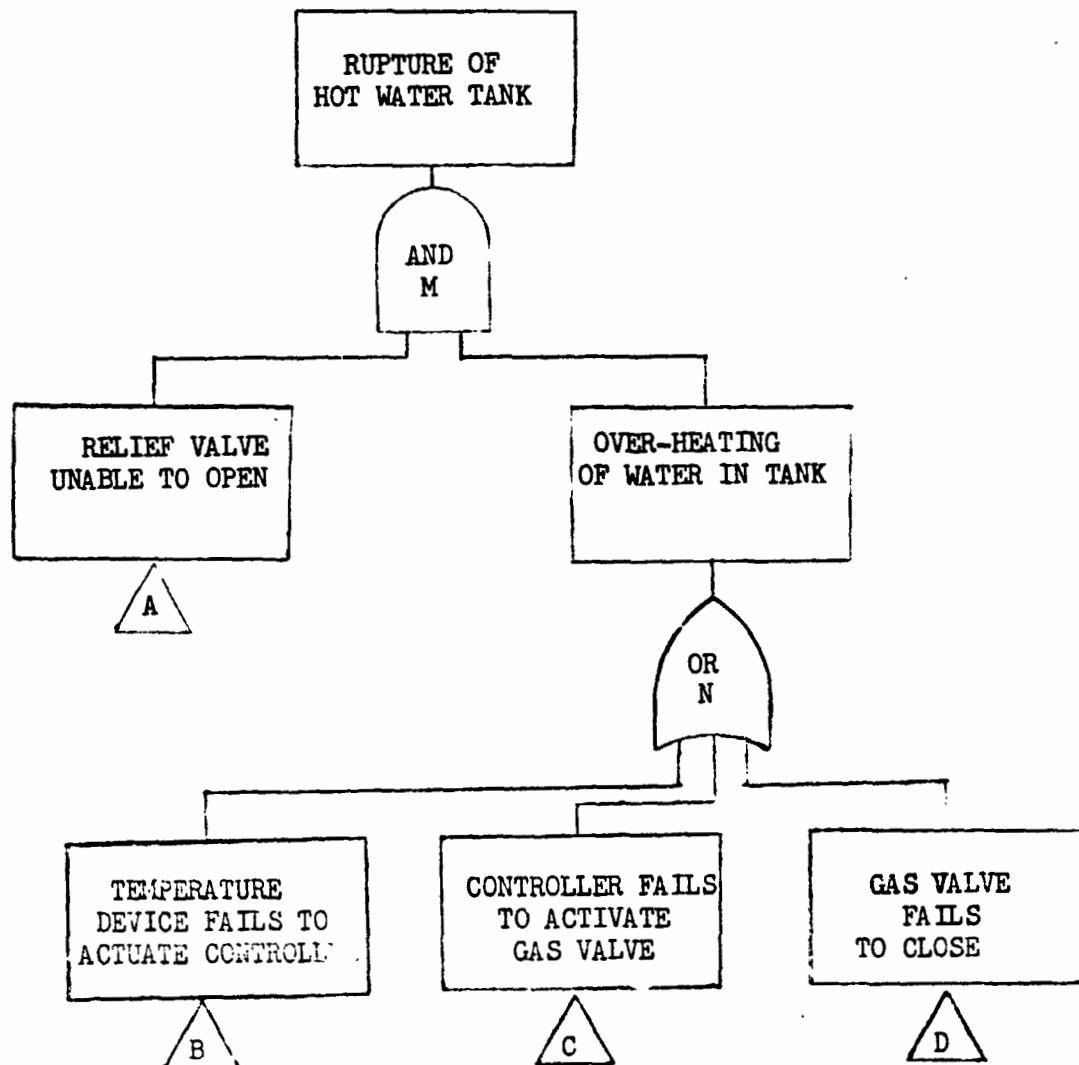


Figure 4-1

4.3.4 (Continued)

Now that the system is understood, we should define our undesired event. This would be the rupture of the hot water tank. Having determined the undesired event, it is necessary to analyze what could cause it. For the tank to rupture, the water in the tank must overheat and the relief valve must be unable to open. It is now necessary to determine what could cause the water in the tank to overheat. Either the gas valve fails to close, allowing gas to flow to the burner, or the controller fails to actuate the gas valve, which would allow gas to flow to the burner, or the temperature device fails to actuate the controller, which also would allow gas to flow to the burner.



Simple Fault Tree
Figure 4-2

4.3.4 (Continued)

The fault tree in Figure 4-2 presents a very simplified analysis. This diagram is a graphic representation of logical relationships, and these may be expressed in Boolean algebra. Only if both event A and event N exist simultaneously, can event M occur. Events A and N have some probability of occurrence, $P(A)$ and $P(N)$ respectively. The probability that M occurs is expressed as, $P(M) = P(A) \times P(N)$.

The fault tree in Figure 4-3 shows that N occurs if any one of the events B, C, or D occur. These events may occur in any combination, but only one must occur to cause event N. The probability of event N is expressed as,

$$P(N) = P(B) + P(C) + P(D) + \left[\overline{P(B)} \times P(C) \times P(D) \right] - \left[\overline{P(B)} \times P(C) + P(B) \times P(D) + P(C) \times P(D) \right]$$

A complete derivation of this equation can be found in most texts on set theory or Boolean algebra.

In most cases, the probability of a failure event is quite small, i.e., in the order of 10^{-2} or less. If 10^{-2} is assumed as an upper limit then;

$$\begin{aligned} P(N) &= 10^{-2} + 10^{-2} + 10^{-2} + \left[10^{-6} \right] - 3 \left[10^{-4} \right] \\ &= 3 \times 10^{-2} - 299 \times 10^{-6} \\ &= 2.9701 \times 10^{-2} \end{aligned}$$

In the approximation, if

$$P(N) = P(B) + P(C) + P(D)$$

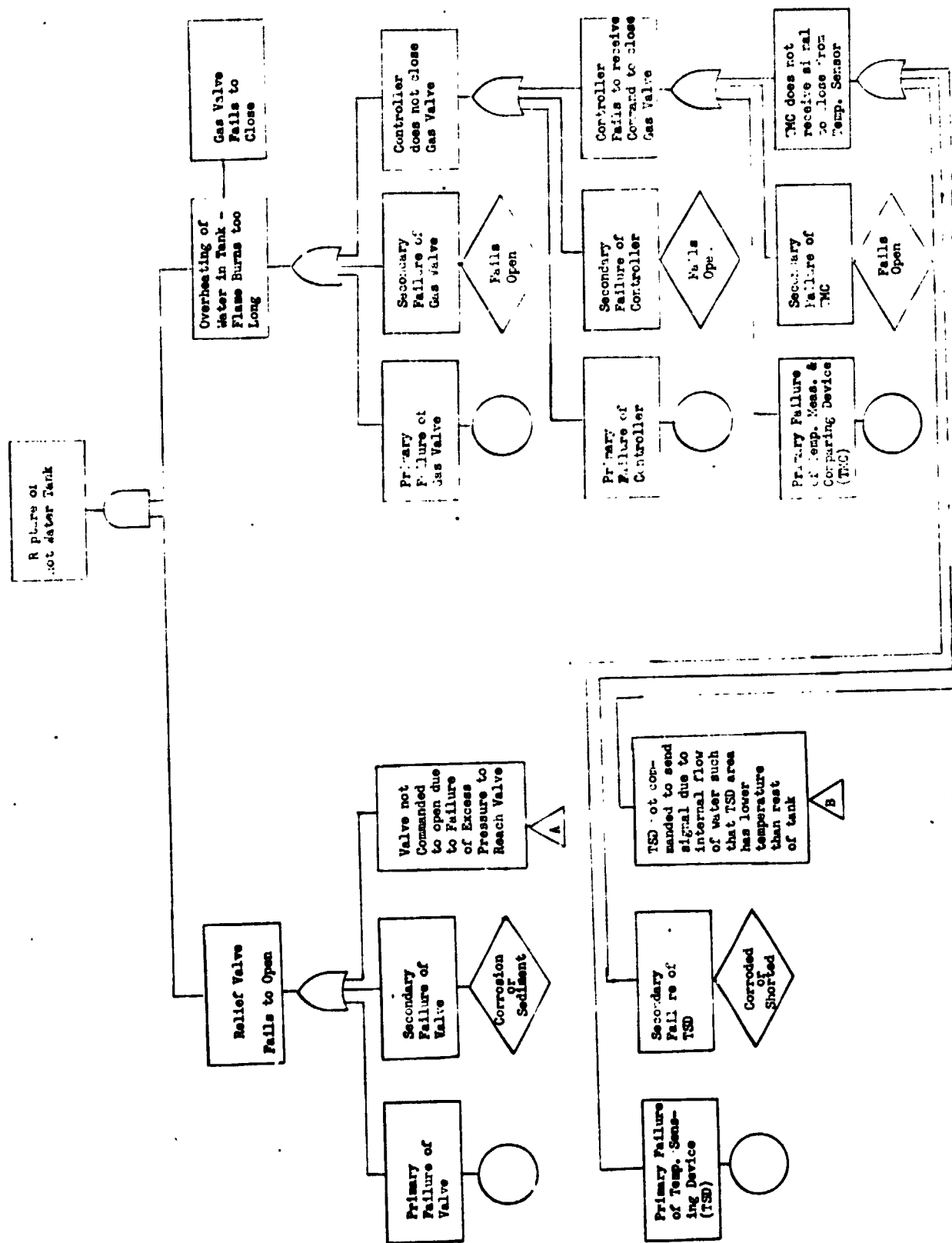
had been used, at most a one percent error would have been introduced. Failure probabilities are normally much smaller than 10^{-2} , and the error of approximation would very likely be much smaller than one percent.

Therefore, a valid approximation of the probability of the top event M is expressed,

$$P(M) = P(A) \times \left[P(B) + P(C) + P(D) \right]$$

Frequently the diagram in Figure 4-2 is all that is needed to lead the analyst to a sound conclusion. On the other hand, if it is necessary to trace out possible faults in each piece of component hardware then the logic diagram might look like Figure 4.3.4B.

USE FOR TYPEWRITTEN MATERIAL ONLY



Expanded Fault Tree
Figure 4-3
Sheet 4-18

4.3.4 (Continued)

A fault tree should be carried down only to the point that one is sure there is no additional significant data to be derived.

It is pointed out, however, that if a quantitative analysis is desired, then the fault tree must be carried to the level of component parts, or subsystems, which have had a failure rate that has been determined by test or analysis. Then by the application of Boolean algebra in combination with other failure probability computation techniques (Lambda-Tau or Monte Carlo), a probability of occurrence of the top undesired event can be calculated.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4 FRACTURE MECHANICS ASSESSMENT (See Appendix D)

4.4.1 Summary Description of Technique

Pressure vessels generally contain small flaws or defects, which are either inherent in the materials or are introduced during a fabrication process. These defects can in many cases cause a severe reduction in the load carrying capability and severely reduce the operational life spans of pressure vessels. If the flaws are large in comparison to that required to cause failure at the proof pressure stress levels, failure will occur during initial pressurization. On the other hand, if the initial flaws are small the vessels may withstand a number of operational pressure cycles and a number of hours of sustained pressure loading before the flaws attain the size needed for failure to occur. From an economic standpoint it is important that the possibility of failure of launch vehicle and spacecraft pressure vessels during proof testing be minimized. From the standpoint of economics and personnel safety, it is imperative that operational failures be prevented.

The primary purpose of this method is to set forth a criteria which, when followed, will minimize the occurrence of proof test failures and provide assurance against pre-flight and flight operational failure of launch vehicle and spacecraft pressure vessels. Within the constraint of "no service failures", the criteria is intended to provide a maximum degree of latitude in the selection of materials and operational stress levels, detail design, analysis, and test in order to allow weight and cost minimization as may be dictated by specific vehicle and mission requirements.

The method is applicable to metallic pressure vessels designed primarily for internal pressure. This includes high pressure gas bottles, solid propellant motor cases, and storable and cryogenic liquid propellant tanks - both integral and removable. Pressurized cabins, inflatable structures and vessels fabricated from composite materials are not included.

The three basic considerations in the prevention of proof test and service failures of metallic pressure vessels are, the initial flaw sizes (K_{I1}), the critical flaw sizes (i.e., the sizes required to cause fracture at a given stress level (K_{I2}), and the subcritical flaw growth characteristics. The prevention of proof test failure is dependent upon the actual initial flaw sizes being less than the critical flaw sizes at the proof stress level. In order to guarantee that the vessel will not fail in service, it is necessary to show that the largest possible initial flaw in the vessel cannot grow to critical size during the required life span. The basic parameters affecting critical flaw sizes are the applied stress levels, the material fracture toughness values, the pressure vessel wall thickness, the flaw location and the flaw orientation. The determination of actual

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4.1 (Continued)

initial flaw sizes is limited primarily by the capabilities of the non-destructive inspection procedures, however, as will be discussed, a successful proof pressure test provides a direct measure of the maximum possible initial flaw size. Subcritical flaw growth depends upon a number of factors including stress level, flaw size, environment, pressure vessel material, and the pressure vs. time/cycle profile.

Because of the many factors involved, it is unlikely that the problem of premature fracture will be completely resolved in the immediate future. However, during the past ten to fifteen years significant progress has been made in several different areas (i.e., mechanics, metallurgy, inspection etc.) with the accomplishments in the field of fracture mechanics being particularly significant. Linear elastic fracture mechanics has provided a basic framework and engineering language for describing the fracture of materials under static, cyclic and sustained stress loading. The technical approach used in developing the criteria set forth in this document is based on this framework.

4.4.2 Application of Fracture Mechanics Assessment

In Aerospace work, systems frequently require use of pressure vessels, both thin walled and thick walled. Because of weight or space restrictions it sometimes is necessary to reduce the normal safety factors used in the design of such vessels.

Experience indicates that small flaws in the vessel structure sometimes cause reactions of a hazardous nature. Pressures used in testing and phenomena associated with the use of gases or chemicals cause the flaws to propagate until damage is effected to the vessel and to the surrounding environment and personnel. This danger can be minimized and predicted by conducting an assessment of the pressure vessel's fracture mechanics characteristics.

4.4.3 Input Data Requirements For Fracture Mechanics

The Fracture Mechanics technique requires that information from systems specifications, diagrams and drawings, manuals, procedures, requirements and history for use in familiarization, evaluation and assessment be provided. Items of information needed include plain stress intensity factors and fracture toughness of the material, including threshold intensity level; the size and shape of the surface flaw; the thickness of the plate; the design operating stress and the proof test stresses; the ultimate strength of the material and yield strength; and data from the procedures pertaining to time and cycles. Hazard and previous failure experience of similar, related and interfacing systems should also be obtained. (See Figure 3-1)

4.4.4 Summary Description of Fracture Mechanics Assessment

This section sets forth some of the criteria for the design of fracture resistant pressure vessels. Fracture specimen tests and fracture mechanics analyses shall be performed for the purposes of predicting critical flaw sizes at the proof and operating stress levels, predicting probable failure modes, determining allowable stress intensity ratios (i.e., K_{I1}/K_{I1c} ratios), determining allowable flaw sizes, and assisting in the determination of allowable design deviations. The specific criteria governing each of these areas are as follows:

4.4.4.1 Critical Flaw Sizes

The critical flaw sizes at the proof and operating stress levels shall be determined for the parent metal and weldments in all high stressed areas of a vessel. Where the total applied stress levels are below the material tensile yield strength, the critical flaw sizes shall be calculated using the appropriate stress intensity equations, the applied stress, and the measured plane strain fracture toughness value (K_{I1c}). Where the total applied stress exceeds the material yield strength, critical flaw sizes shall be empirically determined using fracture specimens which contain flaws that simulate those that can be encountered in the actual vessel.

Prevention of proof test failure requires that there should be no initial flaws in the vessel greater than the critical sizes at the proof stress levels. Accordingly, if the predicted critical flaw sizes are smaller than the sizes which have been demonstrated to be reliably detectable by nondestructive inspection, the vessel design shall be modified so as to increase the critical sizes.

4.4.4.2 Failure Mode Analysis

A failure mode analysis shall be performed for each completed pressure vessel design. The predicted failure mode (i.e., leakage or complete fracture) shall be determined at the proof and maximum operating conditions. Analytical and experimental verification that the probable failure mode is leakage rather than complete fracture shall be required in those cases where assurance of operational life is not provided by the proof test.

4.4.4.3 Allowable Stress Intensities

The performance of cyclic and sustained stress subcritical flaw growth tests of the parent metal and weldments shall be a requirement for all metallic pressure vessels designed for NASA. The resulting data shall be used in conjunction with the maximum expected service life requirements (i.e., cycles, time at pressure, environment, etc.) to determine the allowable initial stress intensity, K_{I1} and allowable stress intensity ratio, K .

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4.4.3 (Continued)

stress intensity, K_{II} and allowable stress intensity ratio, K_{II}/K_{IC} . Because of the major effect that test and service environment can have on sustained stress flow growth every effort shall be made to accurately simulate these environments in the laboratory tests.

For thick walled vessels, the allowable initial stress intensity shall be the largest value which cannot attain the critical value, K_{IC} , due to cyclic and/or sustained stress flow growth within the maximum required life span of the vessel. For both thick and thin walled vessels, which are subjected to prolonged pressurizations, the allowable initial stress intensity shall be less than the sustained stress threshold value, K_{TH} . For vessels which normally experience only one short duration operational cycle (e.g., solid propellant motor cases) the allowable initial stress intensity will be allowed to exceed the threshold values providing that it has been shown from experimental stress intensity versus time data that the initial stress intensity cannot reach the critical value during the operational cycle.

The allowable K_{II}/K_{IC} ratio to be used in determining the proof test factor (App. D) shall be the lowest individual value obtained from the analysis of the subcritical flow growth tests of welds and parent metal in the various anticipated service environments.

4.4.4.4 Allowable Flaws

Any flaws of such size, location, and orientation, which result in an applied stress intensity equal to or less than the allowable initial stress intensity at the operating stress levels, are allowable initial flaws for the vessel as it is placed into service. Using a proof test based on the minimum proof test factor (allowable K_{IC}/K_{II}), the allowable initial flaw sizes will be equal to the critical sizes at proof stress level. To allow for possible flaw growth during proof testing, and thus prevent proof test failure, the allowable initial flaw sizes prior to proof testing shall be somewhat less than the critical sizes at the proof test level. The flaw growth allowance for slow growth during proof testing is dependent upon the material, temperature, and environment and shall be estimated from laboratory test data. Nondestructive inspection acceptance limits shall be evaluated based upon the calculated and experimentally determined allowable flaw sizes. In general, these limits shall be conservative enough to allow for both the uncertainties involved in the determination of allowable flaw sizes and the probable tolerance on the capability of the nondestructive inspection procedures.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4.4.5 Design Deviations

Since design deviations such as radial and angular mismatch of welded joints result in increased stresses which in turn can reduce the allowable flaw sizes, effort shall be made to minimize these deviations. The allowable design deviations for each vessel shall be established based on a study of the resulting stresses, the effect of these stresses on allowable flaw size and nondestructive inspection capability. Joints containing the established allowable radial and angular mismatch and containing the allowable surface flaw (on the high tension stressed surface) shall be able to withstand the proof pressure stresses without failure.

4.4.4.6 Nondestructive Inspection

Pressure vessel weldments and parent metal shall be non-destructively inspected per the applicable inspection specifications called out in the NASA procurement specification for each pressure vessel design. The adequacy of the specified acceptance limits shall be verified based on the allowable flaw size predictions. If the allowable flaw sizes (including the effect of design deviations) are less than the specified acceptance limits, the vessel design shall be modified so as to increase the allowable flaw sizes. The specified acceptance limits shall not be made more restrictive unless it has been clearly demonstrated that the detection of smaller flaws is within the capability of the inspection procedures.

4.4.4.7 Proof Test Procedures

4.4.4.7.1 Test Temperature

Every pressure vessel fabricated shall be proof tested to a stress level equal to or greater than $(1 \div \text{allowable } K_{Ii}/K_{Ic})$ x the maximum operating pressure at a temperature equal to or less than the lowest expected operating temperature, except as noted below.

Where it has been clearly demonstrated from laboratory tests that the pressure vessel weldments and parent metal have increasing plane strain fracture toughness values with decreasing temperature, the vessel shall be tested at a temperature equal to the maximum expected operating temperature.

4.4.4.7.2 Test Fluids

Stress intensity versus time data for the proposed test fluid-pressure vessel material combination shall be obtained prior to performing the proof test. If the threshold stress intensity is low (lower than 0.70), then an alternate less aggressive test fluid shall be used.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4.4.7.3 Pressurization and Hold Times

The time required to pressurize the vessel from K_{TH}/K_{1C} x the proof pressure to the proof pressure level shall be the minimum possible as dictated by the capabilities of the selected pressurization system and shall be maintained for the minimum time possible.

4.4.4.7.4 Depressurization Time

The vessel shall be depressurized from the proof pressure level to K_{TH}/K_{1C} x the proof test level as fast as possible. The exact time to depressurize to this pressure level will depend on the flaw growth rates of material.

4.4.4.7.5 Multiple Cycles

The general criteria is that proof testing shall be limited to a single cycle except in the case where special circumstances dictate the need or make it desirable to conduct more than one proof test. Such special circumstances include the following cases:

- 1) A single proof test cannot be designed to envelop the critical operational pressure, temperature and external loading combinations.
- 2) The vessel has been modified or repaired subsequent to the initial test, and therefore requires recertification of proof test.
- 3) It is desired to extend the guaranteed life of the vessel after it has had a period of service usage.
- 4) From an economical standpoint it is desired to test components (e.g., bulkheads) of the vessel prior to initiating final assembly.
- 5) To minimize the risk of failure at the design temperature, it has been shown (by laboratory experiments on preflawed simulated parts or specimens) that a prior test at a higher temperature is advantageous.

4.4.4.8 Combined Loads

For those pressure vessels which are critical for internal pressure combined with flight loads, it may not be possible to envelop the operational stress levels in the vessel with internal pressure alone. In such cases the proof test setup shall include provisions to apply simulated flight loads combined with internal pressure. These loads shall be applied during the test.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.4.4.9 Post Proof Inspection

While it is possible that small amounts of flaw growth may occur during proof testing, the vessel should not fail in service providing the proof test was properly conceived and executed. Consequently, re-inspection of the vessel subsequent to proof testing is not generally considered to be necessary.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.5 FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS (See Appendix E)

4.5.1 Summary Description of Technique

FMECA considers each functional component of a system in each of its possible failed states, and deduces the effects of such failures on man and the hardware. Data are collected about each component to predict the probability that an actual failure will occur. The failures which have the greatest detrimental effects and which are relatively likely to occur are listed in a safety critical parts list. In this way, attention is focused on the parts of the system which need correction.

FMECA's are conducted in two steps; a Failure Mode and Effects Analysis (FMEA), and a Criticality Analysis (CA). The FMECA should be initiated at the same time that system functional assemblies are being designed. As changes to the design are proposed, these may be incorporated into the FMECA to determine the net effect on system safety.

4.5.2 Application of FMECA

Failure Mode, Effects, and Criticality Analyses (FMECA) have been used for determining the reliability of systems, and may be used to determine system safety also. A different viewpoint is used, however, because the goal of reliability analysis is somewhat different than the goal of safety analysis. The objective of safety analysis is to determine hazards to life and equipment, and the failures that cause the hazards to become damaging.

4.5.3 Input Data for FMECA

Conducting FMECA's requires that system requirements, specifications and drawings be gathered early. If there are trade-off studies completed, these should be reviewed for background in the design compromises being considered. Evaluation of FMECA models requires that large amounts of failure data are gathered and assimilated. (See Figure 3-1)

4.5.4 Procedure for FMECA

The initial step of FMECA is the construction of a logic block diagram showing the functional relationships of the elements of the system under analysis. Next, each component is studied to determine all possible modes of failure. Each failure mode for each component is assumed to occur (the only failure in the system at the instant being analyzed), and the possible effects are traced through the system until the final effect is system damage of a predetermined amount, the injury or death of interfacing personnel, or no perceptible effect on safety. The critical failure modes and components which do affect safety are then studied to determine their failure history. When this is estimated, the probabilities that the safety-affecting effects may occur through each critical component failure mode are calculated.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

SECTION V

REFERENCES

5.0 REFERENCE DOCUMENTATION*

- | | | |
|----|--|---|
| 1 | Apollo Program Directive
APD No. 33 | Center Responsibilities
in the Apollo Program |
| 2 | Apollo Program Directive
APD No. 31 | Apollo System Safety
Program Requirements |
| 3 | Apollo Program Directive
APD No. 26B | Preparation of Test and
Checkout Plans and
Procedures at KSC |
| 4 | Document No. D2-117018-1A
The Boeing Company | "Apollo Logic Diagram
Analysis Guideline" |
| 5 | Drawing No. 10M30111
Rev. A, George C. Marshall
Space Flight Center | Procedure for Performing
Systems Design Analysis |
| 6 | Document No. D2-117019-1,
March 1-68, The Boeing Co.,
Contract NASW 1650 | Guidelines for Operations
and Test Safety Analysis |
| 7 | BSD Exhibit 66-22,
March 1, 1967 | Safety Engineering Analysis
for Field Activities, WS-133 |
| 8 | MIL-HDBK-217A | Reliability Stress and Failure
Rate Data for Electronic
Equipment |
| 9 | MIL-S-38130-A | System Safety Engineering of
Systems and Associated Subsystems
and Equipment, General Requirements
For |
| 10 | Document No. D2-114248-1
The Boeing Company | Fracture Mechanics Assessment of
Apollo Launch Vehicles and Space-
craft Pressure Vessels - Volume I |

*References which may be useful to the system safety engineer in applying specialized techniques of each method are in the respective appendix.

SECTION VI

DEFINITIONS

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 DEFINITIONS

Definitions of particular use to system safety engineers are included herein. Where possible, these definitions have been taken from:

- a. NASA Publication SP-7, "Dictionary of Technical Terminology for Aerospace Use," 1st Edition, 1965.
- b. NASA Publication SP-6001, "Apollo Terminology," August 1963.
- c. Air Force Publication, AFSCM 127-1 "System Safety Management."
- d. NASA Publication, NHB5300.1A, "Reliability and Quality Assurance Program Plan, Apollo"
- e. DOD Publication, MIL-S-38130A, "Safety Engineering of Systems and Associated Subsystems and Equipment, General Requirements for"

ABORT - Premature termination of a mission because of existing or imminent degradation of mission success accompanied by the decision to make safe return of the crew the primary objective.

ACCIDENT - An undesired event occurring by chance and which causes death, injury or damage to property.

ASSEMBLY - A number of parts or subassemblies or any combination thereof joined together to perform a specific function.

CHECKOUT (C/O) - A test or procedure for determining whether a person or device is capable of performing a required operation or function. When used in connection with equipment, a checkout usually consists of the application of a series of operational and calibrational tests in a certain sequence, with the requirement that the response of the device to each of these tests be within a predetermined tolerance. For personnel, the term checkout is sometimes used in the sense of a briefing or explanation to the person involved, rather than a test of that person's capability.

COMPONENT - An article which is a self-contained element of a complete operating unit and which performs a function necessary to the operation of that unit.

COMPONENT AND PART RELIABILITY - A component or part is reliable when it will operate to a predetermined level of probability under the maximum ratings at most severe combination of environments for which it was designed and for the length of time or number of cycles specified.

COMPONENT STRESS - The stresses on component parts are those factors of usage or test which tend to affect the failure rate of these parts. This includes voltage, power, temperature, frequency, rise time, etc; however, the principal stress, other than electrical, is usually the thermal-environmental stress.

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

CREW - A group of ground and flight specialists who perform simultaneous and sequential duties and tasks involved in the accomplishment of an assigned operation.

CREW BAY - Any portion of flight hardware which will be environmentally controlled for crew habitation.

CREW SAFETY - Safe return of crew members whether or not the mission is completed.

CREW SAFETY PROBABILITY - The probability of flight crew return without exceeding prescribed emergency limits.

CREW SAFETY SYSTEM (CSS) - Consists of the necessary sensors, test equipment, and displays, aboard the spacecraft to detect and diagnose malfunctions and to allow the crew to make a reasonable assessment of the contingency. For emergency conditions, the CSS is capable of initiating an abort automatically.

CRITICAL DEFECT - A defect that judgment and experience indicate could result in hazardous or unsafe conditions for individuals using or maintaining the product or could result in failure in accomplishment of the ultimate objective.

CRITICALITY - Assignment of relative importance to hardware or systems.

CRITICALITY PARTS LIST - A listing of those parts whose failure would cause a degradation in mission success or crew safety.

DESTRUCT - The action of detonating or otherwise destroying a vehicle after it has been launched, but before it has completed its course.

DETECTION DEVICES - Sensors used to sense and monitor conditions, e.g., open or closed valves, temperatures, flow rates, etc. The status of the condition is usually displayed on control consoles, such as, Hazard Monitoring Panels.

ENVIRONMENT - The aggregate of all the conditions and influence which affect the operation of equipments and components.

EQUIPMENT - One or more assemblies, or a combination of items, capable of independently performing a complete function.

EQUIPMENT FAILURE - When an equipment no longer meets the minimum acceptable specified performance and cannot be restored through operator adjustment of controls.

FAILURE - The inability of a system, subsystem, component, or part to perform its required function.

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

FAILURE ANALYSIS - The study of a specific failure, which has occurred, in order to determine the circumstances that caused the failure and to arrive at a course of corrective action that will prevent its recurrence.

FAILURE MECHANISM - The physical process which results in a part or equipment failure.

FAILURE MODE - The physical description of the manner in which a failure occurs, the operating condition of the equipment at the time of the failure.

FAILURE MODE, EFFECT AND CRITICALITY ANALYSIS

FAILURE CRITICALITY ANALYSIS - Study of the potential failures that might occur in any part of a space system in relation to other parts of the system in order to determine the severity of effect of each failure in terms of a probable resultant safety hazard, and acceptable degradation of performance, or loss of mission of a space system.

FAILURE EFFECT ANALYSIS - The study of the potential failures that might occur in any part of a space system in order to determine the probable effect of each on all other parts of the system, and on probable mission success.

FAILURE MODE ANALYSIS - The study of a space system and working inter-relationships of the parts thereof under various anticipated conditions of operation (normal and abnormal) in order to determine probable location and mechanism where failures will occur.

FAILURE RATE - Rate at which failures occur as a function of time. If the failure rate is constant, it is frequently expressed as the reciprocal of mean-time-between-failure (MTBF).

FALL-BACK AREAS - Locations in vicinity of launch pad affording blast protection through use of wall, revetments and bunkers or sufficient distance.

FAULT TREE ANALYSIS (LOGIC DIAGRAM ANALYSIS) - A logic oriented graphic representation of the parallel and series combinations of independent personnel or equipment subsystem and component failure and normal operating modes that can result in a specified undesired event. This representation can be quantified to provide a relative measure of the paths leading to these events.

FEASIBILITY STUDY - The phase during which studies are made of a proposed item or technique to determine the degree to which it is practicable, advisable, and adaptable for the intended purpose.

FLIGHT - (1) The movement of an object through the atmosphere or through space, sustained by aerodynamic, aerostatic, or reaction forces, or by orbital speed; especially, the movement of a man-operated or man-controlled device, such as a rocket, a space probe, a space vehicle, or aircraft.
(2) An instance of such a movement.

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

FLIGHT CREW - The Apollo flight crew consists of three men who are cross-trained to be capable of manning any of the Command Module (CM) duty stations. The three crewmen are designated commander, navigator, and systems manager. The CM commander is also the Lunar Excursion Module (LEM) commander.

FLIGHT MISSION - Within a project, the specific technical or scientific objective to be accomplished by a given launching of a space vehicle or launch vehicle.

FLIGHT TERMINATION SYSTEMS - Devices or means for ending flight of space vehicle, e.g., propellant tank rupture, ordnance and explosive separation devices, etc.

GROUND OPERATIONAL SUPPORT SYSTEM (GOSS) - The equipment, excluding the launch vehicle, spacecraft, and launch complex, required to be in operation for direct support of the mission being accomplished. This equipment shall include that used to provide or support mission control, guidance and navigation, tracking, telemetry, communications, logistics, and recovery operations.

GROUND SUPPORT EQUIPMENT (GSE) - That equipment on the ground, including all implements, tools, and devices (mobile or fixed) required to inspect, test, adjust, calibrate, appraise, gage, measure, repair, overhaul, assemble, disassemble, transport, safeguard, record, store, or otherwise function in support of a rocket, space vehicle, or the like, either in the research and development phase or in an operational phase, or in support of the guidance system used with the missile, vehicle, or the like.

The GSE is not considered to include land or buildings; nor does it include the guidance-station equipment itself, but it does include the test and checkout equipment required for operation of the guidance station equipment.

HAZARD - A source of danger or risk.

HAZARDOUS CONDITION - A situation involving risk of injury to personnel or damage to property.

HAZARDOUS OPERATION - Specific operation involving risk.

HOLD-FIRE - An interruption in the countdown previous to ignition for lift-off.

INDUSTRIAL SAFETY - The safety of individual and independent manufacturing processes and industrial materials, equipment, and facilities. Industrial Safety is also that organization which creates and administers safety requirements pertinent to manufacturing or industrial operations, protective equipment, and emergency procedures and equipment. The safety requirements created by Industrial Safety result from: direct observation of industrial activities, accident statistics, bio-medical studies, and equipment and material specifications.

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

INTEGRATED SAFETY PROGRAM - A safety program for assembly, checkout, test, and operation at the Launch Center. This program promotes exchange of information and incorporates safety criteria in procedures and operations that have been developed at other Centers and contractors.

INTERFACE - The junction points or the points within or between systems or subsystems where matching or accommodation must be properly achieved in order to make their operation compatible with the successful operation of all other functional entities in the space vehicle and its ground support.

LAUNCH COMPLEX - That area which contains the space vehicle launching facilities, including the launch pad and servicing structures, the control buildings or blockhouse, propellant transfer equipment, support building, and all other facilities in the immediate vicinity required to support a space vehicle launch or lies within the prelaunch hazard area.

MAINTAINABILITY - The quality of the combined features of equipment design and installation that facilitates the accomplishment of inspection, test, checkout, servicing, repair, and overhaul with a minimum of time, skill, and resources in the planned maintenance environments.

MAINTENANCE - The function of retaining material in or restoring it to a serviceable condition.

MISSION - The objective, task, or purpose which clearly indicates the action to be taken.

MISSION ANALYSIS - A comprehensive evaluation of all the parameters which affect the events of a mission.

MISSION OPERATIONAL SAFETY - The essential safety qualities, considerations, and criteria necessary for a safe mission.

MISSION PROFILE - A graphic or tabular presentation of the flight plan of a spacecraft showing all pertinent events scheduled to occur.

MISSION SUCCESS - The attainment of all or a major part of the scientific objectives of the flight with no crew injury or loss of life. It has sometimes been defined as a safe return of all three astronauts from a completed lunar landing mission.

MISSION TASK - The specified purpose for which a device must perform.

MODULE - (1) A self-contained unit of a launch vehicle or spacecraft which serves as a building block for the overall structure. The module is usually designated by its primary function as command module, lunar landing module, etc. (2) A one-package assembly of functionally associated electronic parts, usually a plug-in unit, so arranged as to function as a system or subsystem;

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

MODULE (Continued) - a black box. (3) The size of some one part of a rocket or other structure, as the semidiameter of a rocket's base, taken as a unit of measure for the proportional design and construction of component parts.

OPERATING TIME - The time period between turn-on and turn-off of a system, subsystem, component or part during which time operation is as specified. Total operating time is the summation of all operating time periods.

OPERATIONS SAFETY ANALYSIS (OSA) - An orderly examination of specified operations (or tasks) with the purpose of identifying significant hazards generated by that operation (i.e., people/machine interface). Each OSA includes those features or preventive measures necessary (Requirements) to eliminate or preclude identified hazards.

OUTGASSING - The release of gasses (when pressure drops) that are entrapped in materials.

PAD SAFETY - That portion of space vehicle safety concerned with vehicle operation in the area of the launch pad. This includes the exercising of precautionary measures on fixed vehicle facilities, ground handling gear on the pad, and the vehicle itself to the point of lift-off.

PART - (1) One of the constituents into which a thing may be divided. Applicable to a major assembly, subassembly, or the smallest individual piece in a given thing. (2) Restrictive. The least subdivision of a thing; a piece that functions in interaction with other elements of a thing but is itself not ordinarily subject to disassembly.

PUBLIC SAFETY - The protection of life and property of people in or close to, but not associated with the whole area of the range.

QUALIFIED MATERIALS - Materials and articles that by determination of tests and examinations of documents and processes verify that materials and articles are capable of meeting performance requirements.

RANGE - Space which is utilized to conduct a launching operation. The Range space for in-flight phase of space vehicle ceases at orbital injection and will vary according to the requirements and characteristics of individual space vehicles and is specifically defined for each mission.

RANGE SAFETY - The process of minimizing hazards to persons or property attendant to space vehicle operations and associated activities. Range Safety includes Pad Safety and Flight Safety.

RANGE USER - An agency having an overall management of a program requiring the use of Test Range facilities in support of space vehicle operations. NASA is a Range User.

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

REDUNDANCY - The existence of more than one means for accomplishing a given task where all means fail before there is an overall failure to the system (NPC 250-1).

Parallel redundancy applies to systems where both means are working at the same time to accomplish the task and when either of the systems is capable of handling the job itself in case of failure of the other system. Standby redundancy applies to a system where there is an alternative means of accomplishing the task that is switched in by a malfunction sensing device when the primary system fails.

RELIABILITY - Of a piece of equipment or a system, the probability of specified performance for a given period of time when used in the specified manner.

RELIABILITY ASSESSMENT - An analytical determination of numerical reliability of a system or portion thereof without actual demonstration testing. Such assessments usually employ mathematical modeling, use of available test results, and some use of estimated reliability figures.

SAFETY - Freedom from those conditions which can cause injury or death to personnel, damage to or loss of equipment, or property.

SAFETY CHECKLIST - A listing for verifying safety aspects of equipment, procedures, and operations.

SAFETY DATA - Recorded knowledge for reference or application in safety and accident prevention field. This includes internal and external directive and procedural information, and safety criteria generated internally and externally such as reports, studies, summaries, panel, and committee minutes.

SAFETY SURVEILLANCE - Observation of designated hazardous/dangerous operations by a safety representative to insure adherence to safety principles, and compliance with operating plans and procedures, technical data, safety directives and checklists.

SPACE SYSTEM - A system consisting of launch vehicle, spacecraft, ground support equipment, and test hardware used in launching, operating, and maintaining the vehicle or craft in space.

SPACE VEHICLE - A launch vehicle and its associated spacecraft.

SUBSYSTEM - A major functional subassembly or grouping of items or equipment which is essential to operational completeness of a system.

SYSTEM - (1) Any organized arrangement in which each component part acts, reacts, or interacts in accordance with an overall design inherent in the arrangement. (2) Specifically, a major component of a given vehicle such

USE FOR TYPEWRITTEN MATERIAL ONLY

6.0 (Continued)

SYSTEM (Continued) - as a propulsion system or a guidance system. Usually called a major system to distinguish it from the systems subordinate or auxiliary to it.

The system of sense 1 may become organized by a process of evolution, as in the solar system, or by deliberate action imposed by the designer, as in a missile system or an electrical system.

In sense 2, the system embraces all its own subsystems including checkout equipment, servicing equipment, and associated technicians and attendants. When the term is preceded by such designating nouns as propulsion or guidance, it clearly refers to a major component of the missile. Without the designating noun, the term may become ambiguous. When modified by the word major, however, it loses its ambiguity and refers to a major component of the missile.

SYSTEM SAFETY - The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of system safety engineering throughout all phases of system development and utilization.

SYSTEM SAFETY ENGINEERING - An element of systems management throughout the program life cycle involving the application of scientific, engineering and management principles for the timely identification of those actions necessary to prevent or control hazards within the system.

TEST - (1) A procedure or action taken to determine under real or simulated conditions the capabilities, limitations, characteristics, effectiveness, reliability or suitability of a material, device, system, or method. (2) A similar procedure or action taken to determine the reactions, limitations, abilities, or skills of a person, other animal, or organism.

WARNING DEVICES - Sensors that monitor or detect conditions and provide visible and/or audible alerting signals as desired for selected events.

ZERO-G CHARACTERISTICS - The reaction or change in behavior of a substance or system introduced into an environment free of gravitational force.

USE FOR TYPEWRITTEN MATERIAL ONLY

APPENDIX A

GROSS HAZARDS ANALYSIS

	<u>Contents</u>	<u>Page</u>
	List of Figures	A-002
1.0	Summary Description of Technique	A-101
2.0	Applications	A-201
3.0	Input Data Requirements	A-301
4.0	Procedure for Gross Hazards Analysis	A-401
5.0	Conclusions	A-501

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix A
List of Figures

Figure No.

Page

A-1 Gross Hazards Analysis Worksheet

A-502

USE FOR TYPEWRITTEN MATERIAL ONLY

APPENDIX A

Gross Hazards Analysis

1.0 SUMMARY DESCRIPTION OF TECHNIQUE

Gross hazards analysis is a comprehensive, qualitative, non-mathematical hazard assessment of a product or system.

The use of gross hazards analysis allows an early assessment of the inherent safety of the completed system. Early design changes, and early procedure changes which are made to eliminate or control hazards minimize costly modification after the system is built. The gross hazards analysis is accomplished in steps as follows:

- 1) Identify all gross hazardous events,
- 2) Prepare functional flows for fault event analysis,
- 3) Evaluate functional flows for fault events or hazards,
- 4) Make design change recommendations,
- 5) Evaluate all procedures for hazards,
- 6) Prepare safety procedures as necessary,
- 7) Evaluate all proposed changes,
- 8) Make design change recommendations on changes,
- 9) Make procedure change recommendations on changes.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0

APPLICATIONS

The gross hazards analysis technique is applicable to complete systems or programs, or to major segments of a system or program, where it is necessary to identify safety critical areas, identify the hazards involved, establish the controlling design criteria that will be used and provide recommendations for hazard elimination or further hazard analysis. The gross hazards analysis allows program management to define the system safety task for the life of the program and plan for manning and budgeting as well as to establish goals and priorities.

USE FOR TYPEWRITTEN MATERIAL ONLY

3.0

INPUT DATA REQUIREMENTS

Data useful for gross hazard analysis studies would include the following:

- 1) Requirement specifications
- 2) System specifications
- 3) Detail specifications
- 4) Flow diagrams
- 5) Schematic diagrams
- 6) Installation drawings
- 7) Detail drawings
- 8) Operations and maintenance manuals
- 9) Technical operating procedures
- 10) Test and checkout procedures
- 11) Test requirements
- 12) Standards
- 13) Waivers and deviations
- 14) Safety codes, procedures and regulations
- 15) Failure reports
- 16) Critical parts lists
- 17) Analyses of similar systems

USE FOR TYPEWRITTEN MATERIAL ONLY

4.0

PROCEDURE FOR GROSS HAZARDS ANALYSIS

1) Operations:

A. Identify all gross hazardous events. Known safety critical areas are identified first using existing design guidelines such as:

1. Company Standards
2. State Codes and Regulations
3. Advisory Codes
4. Range Safety Guidelines.

Considerations in this hazardous events identification would include but not be limited to:

1. Propellants (fuel, oxidizer, mono, solid)
 - (a) Characteristics
 - (b) Hazards - (Personnel, system)
 - (c) Handling Requirements
 - (d) Storage Requirements
 - (e) Transportation Requirements.
2. Explosives
 - (a) Hazard Classifications
 - (b) Characteristics
 - (c) Handling Requirements
 - (d) Storage Requirements
 - (e) Transportation Requirements.
3. Pressure Piping and Vessels
4. Other energy sources in the system.
5. Environmental constraints
 - (a) Radio Frequency Fields
 - (b) Temperature requirements
 - (c) Pressure requirements
 - (d) Vibration requirements
 - (e) Crash worthiness requirements
 - (f) Rescue, Egress and salvage requirements.
6. Operator and Maintainer Human Factors and Training Requirements.
7. Material compatibility
8. Maintainability.
9. Emergency capabilities

USE FOR TYPEWRITTEN MATERIAL ONLY

4.0

(Continued)

Other areas where hazardous conditions are less immediately obvious will require separate analysis and investigation to identify all critical areas.

B. Prepare functional flows for fault event analysis. Major flows might be as follows in a manned flight system. Each major event, system, operation or facility should be identified in the flow.

1. Mission events critical to crew/equipment safety
2. Critical systems
3. Critical operations (manufacturing)
4. Critical operations (test)
5. Critical facilities.

C. Evaluate functional flow diagrams for fault events and hazards.

1. Mission events critical to crew/equipment safety. Events such as the following should be examined to identify potential hazardous conditions.
 - (a) Ground to vehicle power transfer
 - (b) Stages firing and separation
 - (c) Launch escape sequence
 - (d) Ground control and communication
 - (e) In-flight operations and tests
 - (f) Re-entry
 - (g) Recovery.
2. Critical Systems
Systems such as the following should be examined to identify potential hazards.
 - (a) Explosives
 - (b) Propellants
 - (c) Power sources
 - (d) Pressure systems
 - (e) Life-support
 - (f) Propulsion
3. Critical Operations (Manufacturing)
Operations, such as the following, should be examined to identify potential hazards.
 - (a) Toxic or reactive materials
 - (b) Welding
 - (c) Cleaning
 - (d) Handling
 - (e) Fabricating, Forming, Machining
 - (f) Assembly.

USE FOR TYPEWRITTEN MATERIAL ONLY

4:0

(Continued)

4. Critical Operations (Test)

Operations, such as the following, should be examined to identify potential hazards.

- (a) Qualification and Proof Tests
- (b) System Functional Tests
- (c) Explosive Tests
- (d) Transport and Handling
- (e) Static Tests

5. Critical Facilities

Facilities, such as the following should be examined to identify potential hazards.

- (a) Pneumatic
- (b) Propellant
- (c) Assembly
- (d) Ordnance
- (e) Special Test
- (f) Environmental
- (g) Launch
- (h) Manned Item Support.

D. Make design change recommendations.

For each fault or potential hazard, a suitable permanent solution should be proposed for review by design authorities. In some instances a temporary work-around proposal may be necessary to allow further study of a permanent fix.

E. Evaluate all Procedures for Hazards.

- 1. Installation
- 2. Operations
- 3. Maintenance
- 4. Test
- 5. Emergency.

F. Prepare Safety Procedures as Necessary.

- 1. Explosives Control Procedure
- 2. Confined Spaces Entry Procedure
- 3. Radioactive Material Control Procedure
- 4. Toxic Propellant Control Procedure
- 5. Toxic Materials Control Procedure
- 6. Radiographic Operations Procedure
- 7. Flammable Liquids Control Procedure
- 8. Pressure Systems Control Procedure
- 9. Material Disposal Procedure
- 10. Emergencies - Medical - Fire - Explosion
Other
- 11. Other special area procedures.

USE FOR TYPEWRITTEN MATERIAL ONLY

4.0 (Continued)

G. Evaluate All Proposed Changes

As system is modified, redesigned, or updated, the gross hazard analysis of each change should be performed well in advance of change implementation.

H. Make Design Change Recommendations On Proposed Changes.

I. Make Procedure Change Recommendations On Proposed Changes.

2) Documentation of Analysis

Documentation of a gross hazard analysis can take several forms. It should be a working document and may include:

- (a) A list of safety critical systems
- (b) Explosive components list
- (c) Radioactive components list
- (d) Corrective action list
- (e) Work-around action list.

A worksheet useful in summarizing the hazardous condition or conditions, the hazard category designation, and recommendations for action to be taken, including further analysis, for each safety critical item may be patterned after the sample worksheet shown in Figure A1.

5.0 CONCLUSIONS

Gross hazards analysis is generally considered to be a rapid analysis method which will identify areas of concern from a gross standpoint which may then be further analyzed by a more detailed qualitative and/or quantitative technique.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

Program _____		Date of Analysis _____			
System _____		Prepared By _____			
		Checked By _____			
GROSS HAZARD ANALYSIS Work Sheet					
ITEM	SAFETY CRITICAL ITEM	HAZARD DESCRIPTION AND EFFECTS	HAZARD CATEGORY	RECOMMENDED CORRECTIVE ACTION OR FURTHER ANALYSIS	REMARKS
No.	<p>Critical</p> <ul style="list-style-type: none"> -Events -Systems -Subsystems -Operations -Processes -Facilities 	<p>Description of hazardous condition or conditions and effects on program, equipment, or personnel</p>	<p>Assign to one of standard categories</p>	<p>Design or Engineering Change Recommendations</p> <ul style="list-style-type: none"> -Procedure Change Recommendations -Further Analysis Recommendations, i.e., Fault Tree FMECA -Recommendations for Special Tests 	<p>Use for general remarks, follow-up, status notes, etc.</p>

Figure A1

APPENDIX B

OPERATIONS SAFETY ANALYSIS

Contents		<u>Page</u>
List of Figures		B-003
<u>Part I</u>	Operations and Test Safety Analysis (OSA-I)	
<u>Paragraph</u>		<u>Page</u>
1.0	Introduction	BI-101
2.0	Reference Documentation	BI-201
3.0	Analysis Method	BI-301
3.1	Work Sheet	BI-301
3.1.1	Task Column	BI-301
3.1.2	Hazard Column	BI-301
3.1.3	Safety Requirements Column	BI-301
3.1.4	Justification Column	BI-302
3.2	Hazard Determination	BI-302
3.3	Safety Sequence Charts	BI-302
3.3.1	Symbology for Safety Sequence Charts	BI-304
3.3.2	Analysis Reporting	BI-305
3.4	Example of Method (KSC)	BI-307
4.0	Safety Analysis Guide	BI-401
4.1	General	BI-401
4.2	Representative Considerations for OSA	BI-401

USE FOR TYPEWRITTEN MATERIAL ONLY

Contents (Continued)

Operations Safety Research (OSR)

Part II

<u>Paragraph</u>		<u>Page</u>
1.0	Linear Programming	BII-101
1.1	Introduction	BII-101
1.2.1	Measure of Effectiveness	BII-102
1.2.2	Construction of the Linear Model	BII-102
1.2.3	Evaluating the Model	BII-103
1.2.4	Testing the Model	BII-105
1.2.5	Controls	BII-106
1.2.6	Assurance of Control Implementation	BII-106
2.0	Network Analysis	BII-201
2.1	Introduction	BII-201
2.2	Graphic Model	BII-201
2.2.1	Maximum Flow Problems	BII-202
2.2.2	Minimum Path Problems	BII-205
2.2.3	Minimum Spanning Tree	BII-209

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix B
List of Figures

<u>Figure No.</u>		<u>Page</u>
B-1	Test Requirements Data Organization	BI-102
B-2	Work Sheet	BI-303
B-3A	Examples - Symbology	BI-304
B-3B	Examples - Symbology	BI-305
B-4	Safety Sequence Chart	BI-306
B-5	Example - Operations Analysis Format	BI-309
B-6A	Analysis Form	BI-310
B-6B	Analysis Form	BI-311
B-7	Possible Values	BII-103
B-8	Maximum Value	BII-104
B-9	Optimum Value	BII-105
B-10	Graphic Example	BII-201
B-11	Maximal Flow Problem	BII-202
B-12	Network With A Flow Through 1, 2, 4, & 7	BII-203
B-13	Resulting Network With A Total Flow of 17	BII-203
B-14	Network With Minimum Cut Shown	BII-204
B-15	Minimumpath Network	BII-205
B-16	Distance - Node to Node	BII-205
B-17	Step 1	BII-206
B-18	Step 2	BII-206
B-19	Step 3	BII-207
B-20	Step 4	BII-207
B-21	Step 5	BII-208
B-22	Step 6	BII-208
B-23	Step 7	BII-209
B-24	Example Minimum Spanning Tree	BII-210

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix B

Part I

Operations and Test Safety Analysis (OSA-1)

1.0

INTRODUCTION

The Operations and Test Safety Analysis (OSA-1) method identifies operations that are inherently hazardous or, which by the nature of the function sequences, can lead to development of hazards in the operation of a system. This method can be used in all aspects of system operation from construction to mission termination.

The objective of performing OSA's is to ensure that hazards, existing or developing during a particular task, are identified, documented and brought to the attention of the proper authorities for resolution. Such hazards may result from the task itself, or from interaction of other work being done concurrently with the task. The OSA's will include corrective action recommendations which serve to eliminate these hazards, or reduce them to an acceptable level. Each task is reviewed and the reasoning for a particular safety requirement is recorded to substantiate program decisions.

Each task (act, process, or test) shall be analyzed individually to ensure complete investigation of all situations requiring safeguards, special equipment, or specific instructions (e.g., cautions, warnings, or verifications) to avoid personnel injury or significant equipment damage. Previous analyses of hazards in specific areas of operation should be used to the maximum extent. The following method provides a means of accomplishing a comprehensive analysis of each task.

The results of OSA's, specifically safety requirements for each task, can be used as either direct input to the detailed procedures for the task, or can provide a baseline for criteria standards, manuals, or handbooks against which the detailed procedure is written.

Data useful for Operations and Test Safety Analysis would include the following:

- 1) Test and Checkout Plan and Test Requirements

USE FOR TYPEWRITTEN MATERIAL ONLY

1.0 (Continued)

- 2) Test and Checkout Procedure*
- 3) End-to-End Schematics of Test Equipment and Item Being Tested**
- 4) Installation Drawings of Test Equipment

*NOTE 1:

A useful method of organizing this data is to establish a matrix of the equipment components that must be operated and monitored versus the test steps. Each step has requirements as to the configuration of the hydraulic valves, electrical switches or mechanical positions. The safety engineer can then analyze the hazards involved should any element not be in the required mode. See Figure B.1.

**NOTE 2:

Caution should be observed to ensure that schematics reflect all details of the as-built equipment.

CONFIGURATION MODE

Component	REQUIRED TEST STATE					
	1	2	3	4	5	N
Valve AAV #1	Closed	Closed	Open	Closed	Closed	Etc.
Power on Buss #1	Off	On	Off	Off	On	Etc.
Latch #3	Latched	Open	Open	Latched	Latched	Etc.
Relay 6A7	Closed	Open	Open	Open	Open	Etc.
Etc.						

FIGURE B-1 -- TEST REQUIREMENTS DATA ORGANIZATION

2.0

REFERENCE DOCUMENTATION

- | | | |
|---|--|--|
| 1 | Apollo Program Directive
APD No. 33 | Center Responsibilities
in the Apollo Program |
| 2 | Apollo Program Directive
APD No. 31 | Apollo System Safety
Program Requirements |
| 3 | Apollo Program Directive
APD No. 26B | Preparation of Test and
Checkout Plans and
Procedures at KSC |
| 4 | Document No. D2-117019-1,
March 1-68, The Boeing Co.,
Contract NASW 1650 | Guidelines for Operations
and Test Safety Analysis |
| 5 | BSD Exhibit 66-22,
March 1, 1967 | Safety Engineering Analysis
for Field Activities, WS-133 |

USE FOR TYPEWRITTEN MATERIAL ONLY

3.0 ANALYSIS METHOD

3.1 WORK SHEET

The actual analysis may be prepared on a work sheet as shown in Figure B2. It can be prepared in long hand by the analyst and retained for reference. The work sheet should include the following:

3.1.1 Task Column

This column is used to itemize the tasks required to complete the operation or test being analyzed. It should evolve from an examination of every act, function, and associated equipment that is a part of the operation. If new procedures are added by the safety requirements they will also be entered in this column, then analyzed for existing or potential hazards.

In dividing the operation into distinct tasks, the separation must be sufficiently explicit to ensure complete visibility of possible hazards. The task description should include, where appropriate, a brief statement of the function or effect of the operation within the system. Each task will be identified by numbers as shown in Figure B6.

3.1.2 Hazard Column

The Hazards Column contains a description of the hazardous conditions that are revealed by examination of the procedures. It also includes hazards known to exist, although they may already have been resolved. To aid in the search for hazards, identify energy sources and energy transmissions. Use appropriate sequence numbering to correlate the hazards with the correct steps of the procedures (Figure B6). Appropriately indicate those procedural steps in which no hazard can be found. Explain hazards as fully as possible. The questions: what, where, when, how, and why will be answered as applicable. The analyst should consider possible human errors during normal operations and maintenance. Emergency situations should be considered to ensure that such conditions can be mitigated.

3.1.3 Safety Requirements Column

List requirements in procedures, processes, material, or equipment necessary to reduce, or eliminate, the identified hazard(s). If additional tasks are generated by these requirements (Safety Requirements), they can be added to the Task Column. Each of the new tasks must be examined to determine if they create new hazards and subsequent safety requirements. Mandatory sequence of tasks resulting from the analysis can be described in this column.

If sequencing becomes too complex or confusing, a safety sequence chart should be developed to show the prescribed sequence of operation from a safety standpoint. See Figures B3 and B4 for symbols and a sample "Mandatory Safety Sequence Chart", respectively.

USE FOR TYPEWRITTEN MATERIAL ONLY

3.1.4 Justification Column

Pertinent information such as data calculations, standards, ideas, and concepts leading to the identity of a hazard, and the subsequent development of safety requirements are listed in the Justification Column.

Information sources used to determine that a hazard exists and to develop safety requirements must be recorded. This column can list background and reference data such as material specifications, compatibility factors, and logic methods used in arriving at a particular conclusion.

3.2 HAZARD DETERMINATION

Tasks from procedures requirements will be reflected in the Task Column of the OSA. Each of the detailed tasks will be examined to determine functional and nonfunctional relationships with associated equipment, test components, operators, maintenance personnel, and the system as a whole. Based on the elements of each task, any action producing an event or effect that would be detrimental to the system will be identified. This could be developed in general terms of energy control. The analyst will look for such things as uncontrolled, or misuse of mechanical, electrical, electro-magnetic and chemical energies. Springs, levers, pulleys, power supplies, radar antennas, propellants and acids are typical of the many sources of injury to personnel, or damage to equipment. (See Section 4, Page BI-401).

Specific safety requirements will be established to illustrate the need for removing, or effectively reducing, the effects, or potential effects, of uncontrolled energies.

3.3 SAFETY SEQUENCE CHARTS

Development of a Safety Sequence Chart allows easy communication of safety requirements to the operations planning groups. The Sequence Chart further provides a baseline analysis which can be efficiently modified when task objectives are changed, or when identification of new hazards indicates that new operational requirements are desirable.

The safety requirements shown on the Sequence Chart can be indicated on the analysis report sheets in the "Requirements" column and cross referenced for identification on the chart.

Description of the tasks to be accomplished can be found in the test requirements documentation and in the test and checkout plan. If the analysis is conducted late in the operations planning phase, draft test and checkout procedures can provide more information about the equipment involved, and will reflect those safety requirements already established.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

OPERATIONS SAFETY ANALYSIS TASK	OPERATION	LOCATION		JUSTIFICATION
	HAZARDS		SAFETY REQUIREMENTS	

WORKSHEET

Figure B2

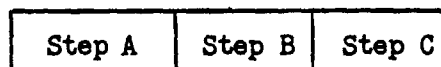
3.3 (Continued)

The Safety Sequence Charts can be developed after all of the tasks are defined, and the required sequence/ parallel accomplishment is based on a knowledge of the hazards in the equipment used.

3.3.1 SYMBOLOGY FOR SAFETY SEQUENCE CHARTS

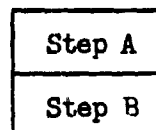
EXAMPLE NUMBER 1

Operations that may be performed in any sequence, but not concurrently:



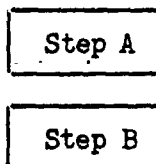
EXAMPLE NUMBER 2

Operations which may be performed concurrently, or consecutively:



EXAMPLE NUMBER 3

Operations which must be performed concurrently:



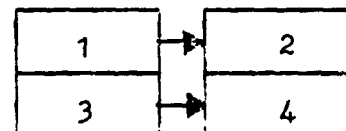
EXAMPLE NUMBER 4

Operations which must be performed in a mandatory sequence: (All operations prior to an arrow must be accomplished before proceeding to next operation.):



EXAMPLE NUMBER 5

Example 5 is a combination of examples 2 and 4:



- Block 1 must be accomplished before Block 2.
- Block 3 must be accomplished before Block 4.
- Blocks 1 and 3 may be accomplished concurrently or in any sequence.
- Blocks 2 and 4 may be accomplished concurrently or in any sequence.
- Block 4 may be accomplished before Block 1.
- Block 2 may be accomplished before Block 3.

Figure B3A

3.3.1 (Continued)

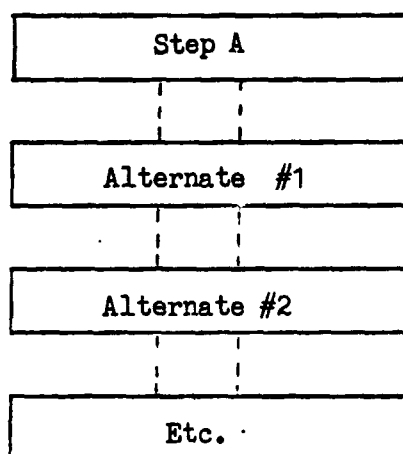
EXAMPLE NUMBER 6

Tasks which have no safety sequencing requirements may be shown as dashed lines:

[- - - -]
[Step X]
[- - - -]

EXAMPLE NUMBER 7

If there are alternate tasks that may be performed to accomplish the same functions, each may need different safety requirements. This may be represented symbolically by:



NOTE: Sequencing requirements must be shown but all possible acceptable sequencing need not be noted.

Figure B3B

3.3.2 ANALYSIS REPORTING

The analysis report may be typed on a form similar to the work sheet excluding the justification column. It should include, however, a correlation column comprised of a notation of where the safety requirement was documented.

Each safety requirement, resulting from the analysis should be provided to the responsible organization before the test so that it can be properly entered in the appropriate document. Inclusion should be identified in the correlation column as step XX of XX-XXXX. If a particular safety requirement is rejected, the Correlation Column should state the reason for its rejection and be forwarded to the center safety office.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

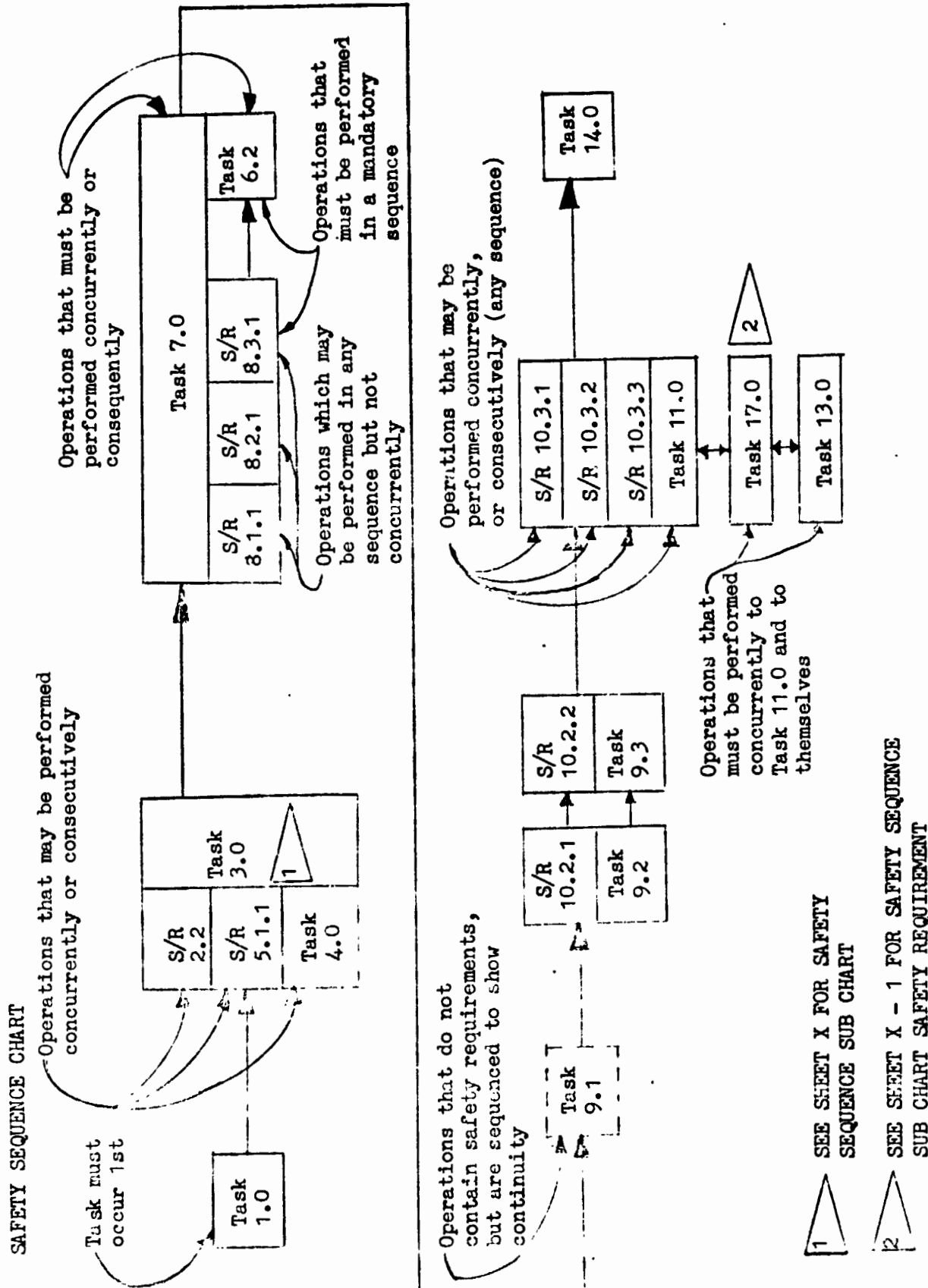


Figure B4

3.4

EXAMPLE OF METHOD (KSC)

The Test and Checkout Requirements document provides the test title and a very brief description of each test. It includes equipment effectivity and pertinent notes advising of certain cautions that must be observed.

The test checkout plan contains an integrated test sequence flow chart showing the overlap, if any, that will occur between the various tests. In the example, (Figure B5 and B6) the Space Vehicle Cutoff and Malfunction Test for AS-503 does not overlap with any preceding or subsequent tests. The T&CO Plan lists each of the tests that will be conducted under this plan by test number (V-20021), stage contractor responsibility code (contractor name), test title (Space Vehicle Cutoff and Malfunction Test), and by the test catalog sheet revision (Rev. A).

The task column of the OSA sheet will be filled in from the Test and Checkout Plan sheet(s), functional flows, drawings, and specifications. Each Act, procedure, or task will be analyzed to determine the possibility of personnel injury or property damage. Each hazard will be described in detail. The safety requirements will tell which action must be taken to prevent the occurrence of the listed hazard. This column will include specific note, caution and warning citations deemed necessary for direct input to detail procedures.

NOTE: A pictorial diagram(s), if available, will be included as applicable in each analysis to define the location(s) of the operation or task being analyzed.

The final analysis sheets (Figure B6) will be formally documented. An Operations and Test Safety Analysis (OSA) will contain:

1) Title Page

Includes analysis number, operation title and signature for preparation and approval;

2) Active Record Sheet

Includes a list of every page in the document with proper identification of added, revised, and deleted pages;

3) Revision Sheet

Will be blank on initial release. Includes a record of added, revised, and deleted pages with a notation telling why change was made. Each revision will require the initials of approving individual.

3.4 (Continued)

Table of Contents

Includes contents of document plus a list of tables, figures, and charts. All tables, figures, and charts will be assigned a figure number beginning with "1" and follow consecutively through the document. Figures are added with subsequent revisions will be: a .1, .2, following the preceding figure number (e.g., 3.1, 3.2, 3.3)

Analysis will include:

Introduction (Figure B5.)

Scope

Summary of Analysis

Ref: Test and Checkout Plan Sheet(s) (Figure B5.)

Test Sequence Flow Plan

Source Material

Operations Sequence Requirements

Equipment (or operation) Location Charts (Figure B5.)

Analysis Sheets (Figure B6)

A document number system will be established at each MSF Center. If numbering systems exist, they will be used as applicable.

USE FOR TYPEWRITTEN MATERIAL ONLY

SAFETY ANALYSIS OF SPACE VEHICLE CUTOFF AND MALFUNCTION TEST - APOLLO/SATURN

1.0 INTRODUCTION

1.1 SCOPE

This document contains the technical safety analysis of test No. V-20021, Space Vehicle Cutoff and Malfunction Test, developed by (name of organization performing analysis) on (date).

1.2 ANALYSIS SUMMARY

This summary shows the most important safety requirements developed in this analysis. They must be implemented before the test. (Describe the effects on the test if requirements are not met. If none, so state.)

2.0 REFERENCES

2.1 TEST AND CHECKOUT PLAN

2.2 TEST SEQUENCE FLOW PLAN

2.3 EQUIPMENT LOCATION CHARTS

2.4 SOURCE MATERIAL

3.0 OPERATIONS SEQUENCE REQUIREMENTS

These are the sequence requirements which result from the safety analysis.

4.0 ANALYSIS SHEETS

USE FOR TYPEWRITTEN MATERIAL ONLY

Example - Operations Analysis Format

FIGURE B5

USE FOR TYPEWRITTEN MATERIAL ONLY

OPERATIONS SAFETY ANALYSIS TASK	OPERATION HAZARDS	LOCATION		CORRE- LATION
		SAFETY REQUIREMENTS		
2.0 Connect power cable in preparation for the Space Vehicle Cutoff and Malfunction Test.	2.0.1 Equipment damage/personnel injury may occur due to exposed voltages.	2.0.1	Visually inspect all electrical cables and connectors for physical damage.	
	2.0.2 Equipment damage/personnel injury may occur due to improper voltage.	2.0.2	Verify that all voltage sources to be used in this test are within tolerance.	
	2.0.3 Equipment may be improperly operated by unauthorized personnel.	2.0.3	Verify that only authorized personnel are present during this test.	
2.1 Disconnect C1-J1 from P-2 of the umbilical "in" box.	2.1.1 Equipment damage/personnel injury may occur due to disconnecting cable with power applied.	2.1.1	Verify power has been removed from cable C-1 at J-2.	
	2.1.2 Connectors may be damaged if not protected.	2.1.2	Install dust cover on connector J-2 of cable C-1.	

USE FOR TYPEWRITTEN MATERIAL ONLY

OPERATIONS SAFETY ANALYSIS	OPERATION	LOCATION	CORRE- LATION
TASK	HAZ	SAFETY REQUIREMENTS	
2.2 Connect C2-J2 to P-7 of the ground power "J" box.	2.2 Equipment damage/personnel injury may occur.	2.2 Verify that S-1 through S-12 of ground power "J" box are in the "OFF" position.	
2.3 Connect C2-J1 to P-2 of the umbilical "J" box.	2.3 Spurious or inadvertent voltages may cause equipment damage.	2.3 A hazardous current test shall be conducted at C2-J1 immediately prior to connecting C2-J1 to P-2 of the umbilical "J" box.	
		<div>CAUTION S-1 through S-12 of the Ground Power "J" Box shall remain in the "OFF" position for this entire operation.</div>	

4.0 SAFETY ANALYSIS GUIDE

4.1 GENERAL

The following guide, containing hazards to be considered during the analysis of a task, is only a partial listing and represents the type of areas to be questioned. It is not practical to attempt a comprehensive list of all possible conditions or hazards attendant for a given test before completing the analysis. The prime factor in accomplishing an operation and test safety analysis is knowledge of the equipment involved and its relationship to the surrounding equipment or system.

4.2 REPRESENTATIVE CONSIDERATIONS FOR OSA

- 1) Consider special safety barrier requirements for modification work;
- 2) Determine grounding or disconnection requirements for work on electrical/electronic equipment;
- 3) Determine that operation in one area, or on one item of equipment, will not create or induce a hazard in another area, or on associated items of equipment;
- 4) Consider special or additional lighting requirements for modification work;
- 5) Consider need for special personnel protective clothing and equipment (e.g., safety harnesses, breathing apparatus, or goggles);
- 6) Consider all hazards associated with welding operations (e.g., transient currents, electrical interference, fire and air contamination);
- 7) Consider the need for special ventilation requirements for personnel working in closed area, oxygen deficient conditions, or in contaminated air (e.g., inside, tanks, or performing painting, welding, or cleaning operations);
- 8) Consider dangers associated with personnel working in proximity to high voltage;
- 9) Consider the need for backup power when working on primary power source;
- 10) When drilling or chipping concrete, investigate the possibility of contacting or damaging embedded pipe or conduit;

USE FOR TYPEWRITTEN MATERIAL ONLY

4.2 (Continued)

- 11) Determine the probability of any task restricting egress from the work area by blocking passageways or doors with equipment;
- 12) Investigate hazards associated with installation and removal of explosive ordnance devices and electrical connection to, or disconnection from, ordnance devices;
- 13) Consider the need for special retest instructions;
- 14) Consider the need for special entry/exit procedures;
- 15) Ensure that provisions have been made to communicate with personnel in isolated areas;
- 16) Review requirements for warning placards;
- 17) Consider safety precautions to be observed by personnel working on or around exposed electrical equipment;
- 18) Consider the hazards involved when personnel are working around caustic, poisonous, or cryogenic materials;
- 19) Establish special precautions for connecting or disconnecting cables;
- 20) Consider electrical interference hazards stemming from use of electrical powered tools;
- 21) Consider the effects of status monitoring, or communications interruptions;
- 22) Determine if special procedures are required to prevent induced faults when working on primary power equipment and switchgear;
- 23) Consider requirements for equipment isolation when working on electrical or electronic power equipment.

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix B

Part II

OPERATIONS SAFETY RESEARCH

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix B

Part II

OPERATIONS SAFETY RESEARCH

1.0 LINEAR PROGRAMMING

1.1 INTRODUCTION

Linear Programming has had a wide variety of uses, but a common characteristic for all has been the optimum allocation of limited resources to accomplish a defined objective. The optimal combination of operations minimizes cost, period of performance, system output errors, number of operations required, number of operators required, and is least likely to cause system damage or personnel injury. The resources used to operate a system can be allocated so as to optimize system safety.

1.2 DESCRIPTION OF THE LINEAR PROGRAMMING METHOD

Linear Programming is a mathematical model which describes a characteristic of a system. For system safety engineers, this characteristic is operational safety. Use of this method requires that all mathematical functions in the model must either be, or closely approximate linear, or be closely approximated by linear functions. Use of the model allows the programming, or planning, of activities to obtain the optimum level of safety.

Linear programming is generally divided into six steps:

1. Define the measure of effectiveness,
2. Construct the model,
3. Evaluate the model for optimal results,
4. Test the model and it's solution,
5. Define the controls to ensure optimum results, and
6. Assure that controls are implemented.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.2.1 Measure of Effectiveness

The operational safety problem may be stated in two ways;
 (a) The degree of safety may be chosen, in which case the solution of the math model should be maximized. (b) If risk is chosen as the measure of effectiveness, the solution of the linear model must be minimized. Note: For the discussion that follows, risk will be assumed as the measure of effectiveness.*

1.2.2 Construction of the Linear Model

It is necessary to find the values of the variables $x_1, x_2, x_3 \dots x_n$ which minimize the function of risk

$$R = c_1 x_1 + c_2 x_2 + \dots c_n x_n.$$

Where x_i could be the hazard associated with each resource consumed, and c_i is the increase in r for each unit of x_i .

Constraints on the variables take the form of inequalities

$$a_{11}x_1 + a_{12}x_2 + \dots a_{1n}x_n \geq b_1$$

$$a_{21}x_1 + a_{22}x_2 + \dots a_{2n}x_n \geq b_2$$

$$a_{m1}x_1 + a_{m2}x_2 + \dots a_{mn}x_n \geq b_m$$

and;

$$x_1 \geq 0, x_2 \geq 0, \dots x_n \geq 0.$$

The limits $b_1, b_2, \dots b_m$ can be the total available resources for the achievement of the task objective. This could be total manpower, pounds of propellant, electric power generation capability, etc.. The coefficients $a_{11}, a_{12}, \dots a_{mn}$ are the units of each resource consumed by each unit of hazard. For example, a_{1j} could be the BTU's per pound of propellant, TNT explosive energy equivalency per pound of propellant, or amperes available at man-machine interfaces per watts of power available at the test equipment. The specific units of a_{ij} depend on the hazard, x_i , and the resource b_j .

*Each time the system is operated, there are two possible outcomes. One is that the tasks are performed without any equipment damage or personnel injury. The other outcome may be that some injury or damage occurs. The probability of safe performance (i.e., no damage, etc.) is $P(S)$, and the probability of an accident is $P(A)$. $P(A)$ is the risk, and $P(S) = 1 - P(A)$.

1.2.3 Evaluating The Model

The most common method of solving linear programming problems is the Simplex Method. To illustrate this method, assume the linear model,

$$Z = 3x_1 + 5x_2$$

with constrictions,

$$x_1 \leq 4$$

$$x_2 \leq 6$$

$$3x_1 + 2x_2 \leq 18$$

$$x_1 > 0, x_2 > 0.$$

The possible values of (x_1, x_2) coordinates are shown below.

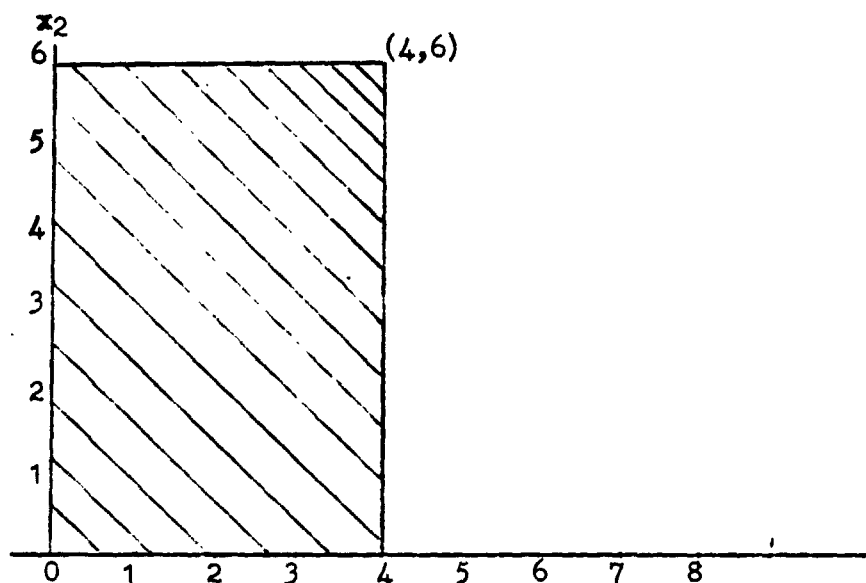


Figure B-7 - Possible Values

The shaded area represents all possible combinations of x_1 , and x_2 which satisfy the inequalities $x_1 \leq 4$ and $x_2 \leq 6$.

1.2.3 (Continued)

Adding the maximum of the constraint $3x_1 + 2x_2 \leq 18$ yields the shaded domain shown below.

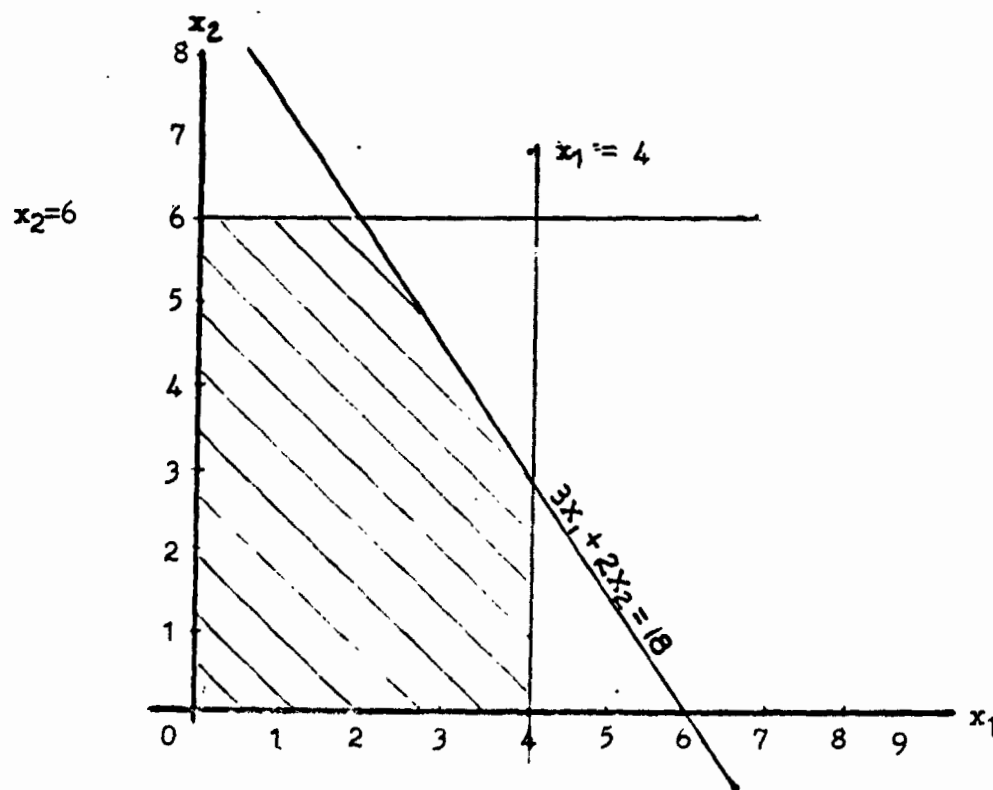


Figure B-8 - Maximum Value

The maximum value for the objective function,

$$Z = 3x_1 + 5x_2$$

exists in this domain, and could be found by trying some values for Z . If Z is 20, the line $20 = 3x_1 + 5x_2$ lies well inside the domain, and there are many pairs (x_1, x_2) which satisfy the constraints and the objective function. Z must be higher in value. The optimum value will have only one pair (x_1, x_2) which will solve the linear function.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.2.3 (Continued)

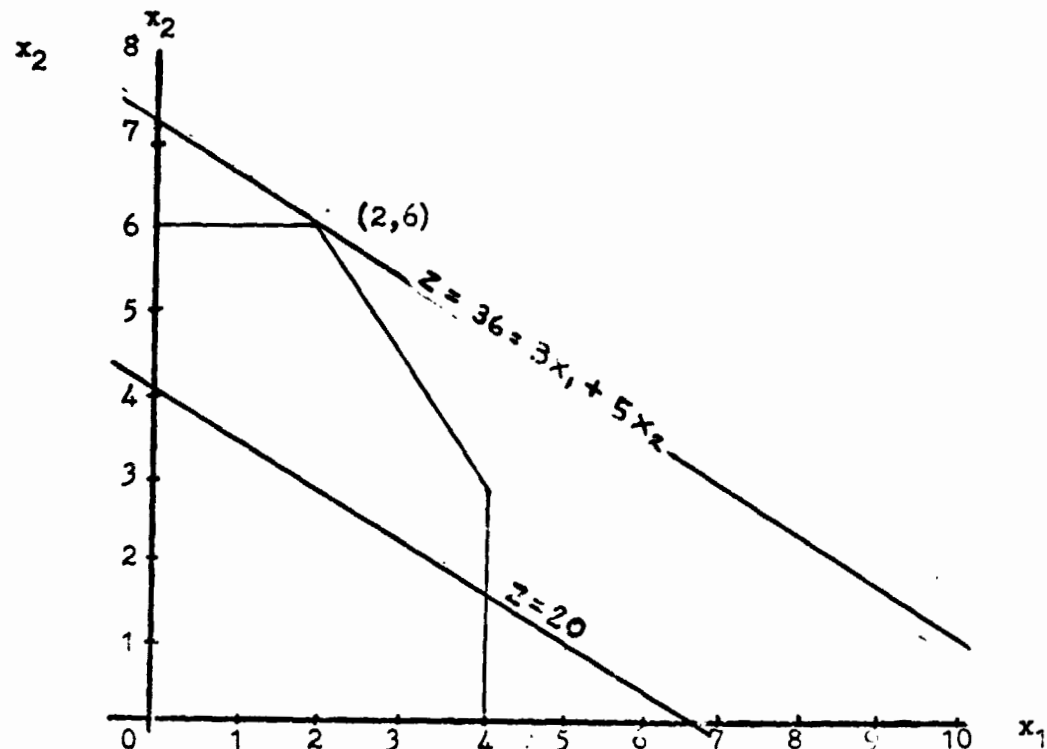


Figure B-9 - Optimum Value

The value of Z which is the optimum is $36 = 3x_1 + 5x_2$; and $x_1 = 2$, $x_2 = 6$ are the desired values for the input variables which will produce the optimum.

It is feasible to use the graphic approach for linear program solution with up to three decision variables, x_1 , x_2 , and x_3 . Most objective functions will have more than three variables and the solution can be found by use of a computerized Simplex Method. The solution by computer is more complex than illustrated in the above example; however, most texts on Operations Research will provide the details of determining the optimal solution by means of this method.

1.2.4 Testing The Model

Test the particular linear model and the optimal solution that has been determined to ascertain if it predicts safety or risk for each alternative combination of operations with sufficient accuracy to permit valid decisions. If at all possible, use historical data for the system under study to simulate past operations which have known outcomes (i.e., accidents, incidents, or safe operation). Compare these outcomes with the results using the linear model with the historical data substituted into the objective function. Much care should be exercised to assure that the constraints derived for the system at present were true when the historical data was generated.

1.2.5 Controls

Define the controls on the system operation which the linear program indicates have a bearing on optimizing safety. Controls may take the form of safety standards or safety operating criteria. The requirements that certain operations must occur in series, in some ordered sequence, or concurrently form controls which can optimize safety.

1.2.6 Assurance of Control Implementation

When systems managers impose the recommended controls, monitor the system operations to determine that they do in fact tend to reduce risk. Review of accident and incident reports before and after the controls were implemented may be helpful. Direct communication with the system operators is virtually essential throughout an entire linear programming analysis, and is especially beneficial during the assurance phase.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 NETWORK ANALYSIS

2.1 INTRODUCTION

Network Analysis has been applied very successfully for increasing the efficiency of manufacturing processes, decreasing the handling and shipping delays encountered in product distribution systems, and maximizing the probability of meeting program schedules. The method is very general and fundamental to the simulation of systems or combinations of operations. Applications may be possible for system safety analysis if analogies can be made between appropriate system characteristics and the concepts of flow and path length. For example, the object of an emergency egress system is to evacuate as many people as possible in the shortest time possible, and in the safest possible way. The latter objective considers the vulnerability of the escapees to the accident created environment (heat, pressure, etc.) as well as the inherent safety of the egress system in use. The analysis of such an egress system would require three networks: one to maximize the flow of people; one to minimize path lengths from work stations to the defined safe area; and one to minimize vulnerability of the escapees within the constraints of each possible accident in the work area. The optimum network must then be chosen, using the method of Linear Programming if necessary.

The following paragraphs will summarize the network model and three uses of the method to optimize flow, path length, and path alternatives.

2.2 GRAPHIC MODEL

The representation of the real system or set of physical operations used in Network Analysis is a graph consisting of junctions, called "nodes" and connection lines called "branches". The junctions represent functional points in the system and the branches indicate the existing interfaces or interdependancies of the functional points. If a flow is associated with each branch, the graph is considered a "network". In the graph example the junctions are circles and the branches are the interconnecting lines. A "chain"

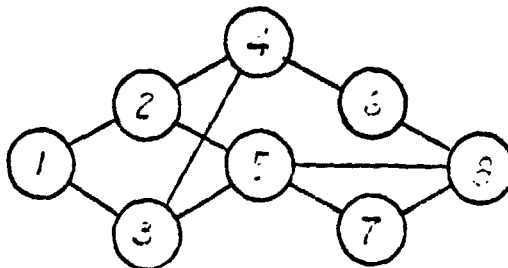


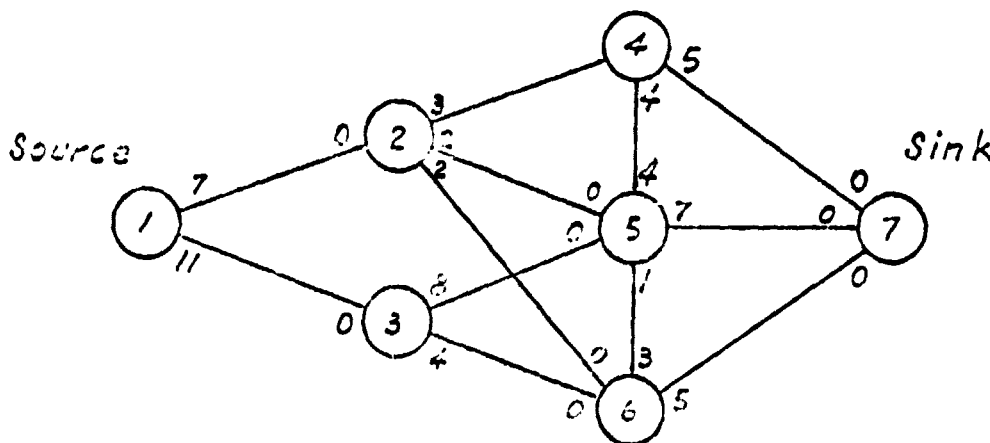
Figure B-10 - GRAPH EXAMPLE

2.2 (Continued)

is a series of nodes and branches that connect each pair of nodes. For example, one possible chain between 1 and 8 is (1,2), (2,4), (4,6), (6,8) or the reverse (8,6), (6,4), (4,2), (2,1). If a direction of flow through the chain is specified, it is called a "path". A chain connecting a node to itself is termed a "cycle". A graph for which every pair of nodes are connected through a chain is called a "connected graph". A connected graph which does not contain any cycles is a "tree". One graph theorem states that a graph containing n nodes is connected if it has $(n-1)$ branches and no cycles. Such a graph would also be a tree. A branch is "directed" if a sense of direction is associated with it so that the node at one end can be considered a source and the node at the opposite end can be interpreted as a sink. A connected graph in which all branches are directed is a "directed graph". If a directed graph is a network, the direction is assumed to be the feasible direction of flow in each path. A network is not directed if flow can occur in both directions along one or more paths. The "capacity" of flow is the maximum feasible flow in one direction. Capacity can be any non-negative number from zero to infinity. If capacity in one direction along a path is zero, the branch is directed. If all paths connected to a node are directed away from the node, it is a source. If all of the connected paths flow into the node, it is a sink.

2.2.1 Maximum Flow Problems

Consider a network with a source at one end and a sink at the other, and assume no loss of flow at each intermediate node. The object is to determine the feasible steady state flow pattern which maximizes the flow from the source to the sink.



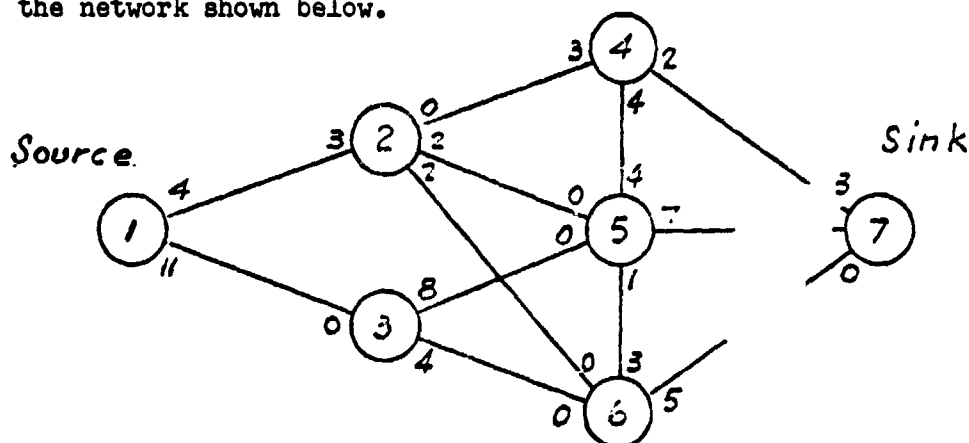
MAXIMAL FLOW PROBLEM

Figure B-11

2.2.1 (Continued)

The flow capacity is indicated for each path by the node from which the flow enters the path. For example, the flow from 1 to 2 can be 7, but the flow capacity from 2 to 1 is zero. The solution of the network is accomplished by the iterative process of assigning and reassigning a feasible flow for each chain from the source to the sink until the positive flow capacity has been used in each chain. The total flow obtained this way will be optimal, but is not necessarily the only optimal flow pattern.

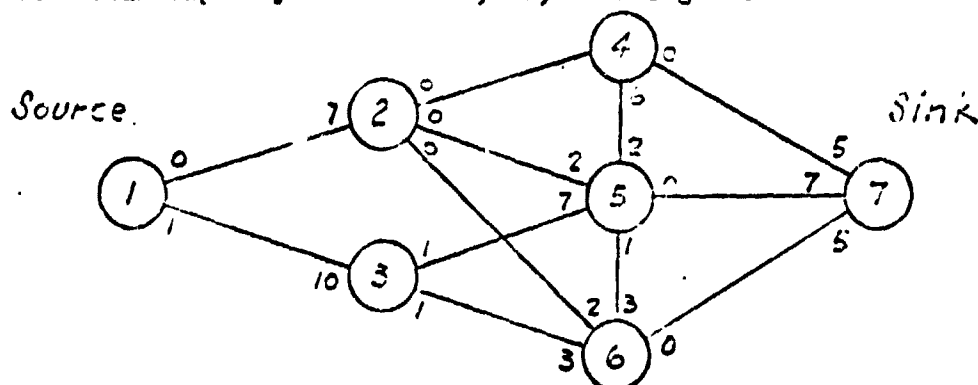
One possible flow in the example is 3 along the chain 1, 2, 4, 7. Since only net flow through a path is significant, it is possible to assign fictitious negative flows in the reverse direction. The remaining capacity in each path of the chain is found by decreasing the positive flow capacity on each path by the assigned flow value of the smallest capacity along the chain. The example then becomes the network shown below.



NETWORK WITH A FLOW OF 3 THROUGH 1, 2, 4, & 7

Figure B-12

Assign a flow of 7 through 1, 3, 5, 7; a flow of 2 through 1, 2, 5, 4, 7; a flow of 2 through 1, 2, 6, 7; and a flow of 3 through 1, 3, 6, 7. The resulting network is optimal in this case, since the total capacity of the sink, 17, is assigned.

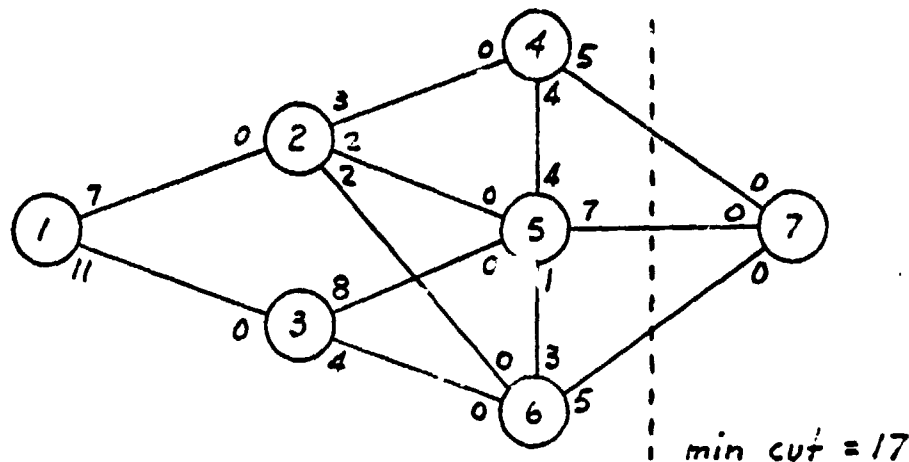


RESULTING NETWORK WITH A TOTAL FLOW OF 17

Figure B-13

2.2.1 (Continued)

This is a special case of the "max-flow min-cut" theorem which states that, for any network with a single source and sink, the maximum feasible flow from source to sink equals the minimum cut value for all the cuts of the network. A minimal cut is shown below. From the theorem, the value of any cut provides an upper bound to the flow, and the least upper bound would then be the maximum possible flow.



NETWORK WITH MINIMUM CUT SHOWN

Figure B-14

Had the minimum cut been recognized at the beginning, the solution process could have been shortened, and each chain would not have to be worked out.

When networks become complex, it is desirable to shorten the solution by use of the computer. This may be done by programming the computer to sum successive cuts through the network until the minimum cut is found, or by having the computer solve the feasible chains and assign flows until no positive flow capacity is left in the network.

A correlation to the emergency egress problem may be made in which the source is the location of the escapees at the time of the alarm. The network represents the alternate routes that the people may choose, and the sink may be the point at which a safe environment is available. This problem closely represents an escape situation where medical or rescue teams must stay together during escape.

2.2.2 Minimum Path Problems

Consider the connected network shown below in which the length of each branch is known. The object is to determine the shortest route from the origin to the terminus.

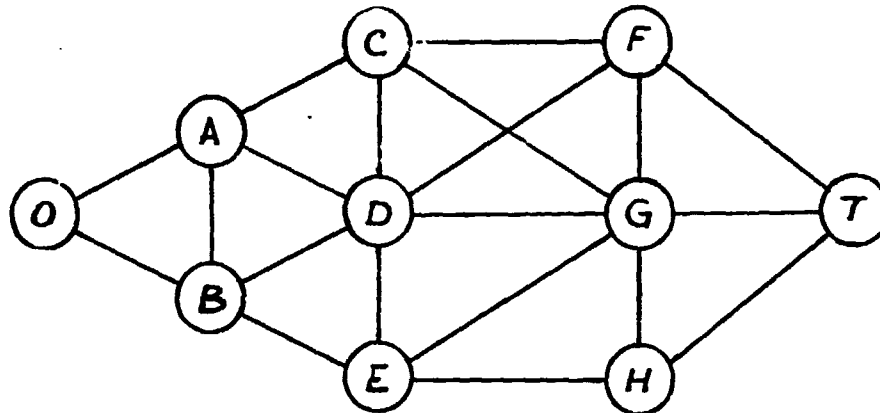


Figure B-15 - Minimum Path Network
The shortest method of finding the minimum path is to start at the origin and successively select the shortest paths to the adjacent nodes in ascending order of their distances. When the terminus is reached, the shortest path should be identified.

The distance from node to node is shown below in tabular form.

NODE	O	A	B	C	D	E	F	G	H	T
BRANCH- LENGTH	OA-7	AD-6	BE-4	CD-2	DC-2	EB-4	FD-2	GC-3	HE-6	
	OB-8	AB-7	BD-6	CF-3	DF-2	EH-6	FC-3	GF-5	HG-8	
		AC-8	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				CA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
					DE-7			GE-9		

Figure B-16 - Distance Node to Node

Step 1: The shortest distance to the closest adjacent node is 7 to A. Circle OA-7, write 7 over A node's column,

2.2.2 (Continued)

cross out the branches leading to A, as shown below.

NODE	7									
	0	A	B	C	D	E	F	G	H	T
BRANCH- LENGTH	<u>OA-7</u>	AD-6	BE-4	CD-2	DC-2	EB-4	FD-2	GC-3	HE-6	
	OB-8	AB-7	BD-6	CF-3	DF-2	EH-6	FC-3	GF-5	HG-8	
		AC-8	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				EA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
					DE-7			GE-9		

Figure B-17 - Step 1

Step 2: The candidates for the next nearest nodes to A and O are B and D. The comparison of distance from O yields 8 for B and 13 for D, so select B. Circle OB-8, write 8 above B node's column and cross out all branches leading to B. Circle the node column when all choices have been considered.

NODE	7 8									
	<u>O</u>	A	B	C	D	E	F	G	H	T
BRANCH- LENGTH	<u>OA-7</u>	AD-6	BE-4	CD-2	DC-2	EB-4	FD-2	GC-3	HE-6	
	<u>OB-8</u>	AB-7	BD-6	CF-3	DF-2	EH-6	FC-3	GF-5	HG-8	
		AC-8	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				EA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
					DE-7			GE-9		

Figure B-18 - Step 2

Step 3: Candidates for nodes closest to O and B are D and E. The shortest route from O to D is $7 + 6 = 13$ through A, and the distance to E from O is $8 + 4 = 12$ through B. Select E and change the list as below.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.2.2 (Continued)

NODE	①	7	8			12				
		A	B	C	D	E	F	G	H	T
BRANCH- LENGTH	①A-7	AD-6	①B-4	CD-2	DC-2	DE-4	FD-2	GC-3	BE-6	
	①B-8	AB-7	BD-6	CF-3	DF-2	EH-6	FG-3	GF-5	HG-8	
		AC-8	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				CA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
					DE-7			GE-9		

Figure B - 19 - Step 3

Step 4: The distance to D from O through A is 13 and through B is 14, and from O to H through E is $12 + 6 = 18$. Select D because it is the closest to both E and O. (G is not a candidate because of the length 9 from EG and the length from O to G compared to O to H or O to D).

	7	8		13	12					
NODE	(O)	A	(B)	C	D	E	F	G	H	T
BRANCH- LENGTH	(OA-7)	(AD-6)	(BE-4)	CD-2	DC-2	ED-4	FD-2	GC-3	HE-6	
	(OB-8)	AB-7	BD-6	CF-3	DF-2	EH-6	FC-3	GF-5	HG-8	
		AC-8	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				CA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
				DE-7				GE-9		

Figure B-20 - Step 4

Step 5: Candidates for new nodes closest to both D and O are C, F, and H. The distance to C from O is $7 + 8 = 15$ through A. The shortest distance to D from O has been shown in step 4 to be 13, so the distance to C and F through D is $13 + 2 = 15$ in both cases. The shortest distance to H is through E. The distance OH is then $12 + 6 = 18$. Nodes C and F are equidistant, so select both. Use the chain OAC or OADC since the distances are equal. The modified table is shown below. When looking at C cross out all paths into C, other than from A or D and then looking at F cross out paths to it other than from D.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.2.2 (Continued)

		7	8	15	13	12	15			
NODE	(O)	(A)	(B)	C	D	E	F	G	H	T
BRANCH- LENGTH	(OA-7)	(AD-6)	(BE-4)	CD-7	(DC-2)	ED-7	FD-2	GD-3	HD-6	
	(OB-8)	AB-7	BD-6	CB-3	(DF-2)	EH-6	FG-5	AG-5	HG-8	
		(AC-8)	BA-7	CG-3	DA-6	ED-7	FG-5	GD-6	HT-8	
				CA-8	DB-6	EG-9	FT-9	GH-8		
					DG-6			GT-8		
					DE-7			GE-9		

Figure B-21 - Step 5

Step 6: New nodes closest of O and C are F and G. Path CF has been eliminated in step 5, but G is still a candidate. The distance to G from O through C is $15 + 3 = 18$, and through D is $13 + 6 = 19$. The path from O to H through E has not yet been eliminated, and it ties with the other OACG path at $12 + 6 = 18$. Because of the equality select both node G (through C) and node H.

		7	8	15	13	12	15	18	18	
NODE	(O)	(A)	(B)	(C)	(D)	(E)	F	G	H	T
BRANCH- LENGTH	(OA-7)	(AD-6)	(BE-4)	CD-7	(DC-2)	ED-7	FD-2	GD-3	HD-6	
	(OB-8)	AB-7	BD-6	CB-3	(DF-2)	(EH-6)	FC-3	GA-5	HG-8	
		(AC-8)	BA-7	(CG-3)	DA-6	ED-7	EG-5	GD-6	HT-8	
				CA-8	DB-6	EC-9	FT-9	GH-8		
					DC-6			GT-8		
					DE-7			GE-9		

Figure B-21 - Step 6

Step 7: Consider nodes F, G, and H. The next new node is T, the terminus. The distances through F, G, and H to T are $15 + 9 = 24$ for F; $18 + 8 = 26$ for G; and $18 + 8 = 26$ for H. The shortest path is, therefore, through F. The final table appears below. The minimal path through the network is identified and is O,A,D,F,T.

2.2.2 (Continued)

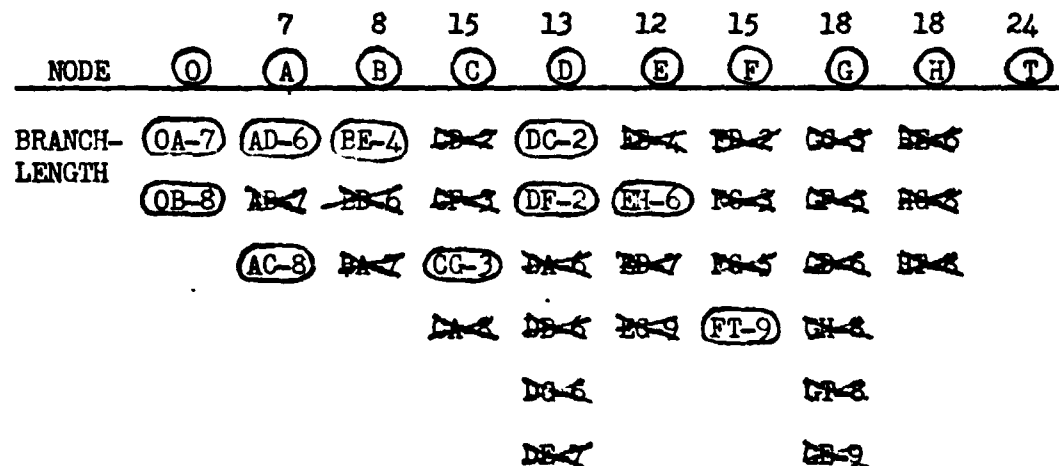


Figure B-23 - Step 7

The correlation of the minimum path network to the emergency escape problem depends on the assumption that the egress rate (or the velocity of the escapees) is the same for all paths. The objective is to select the shortest, and, therefore, the fastest path to the safe place at the terminus. The escape rate may not be equal for all paths. In this case, use time instead of distance to select the quickest path, which may not be the shortest in distance.

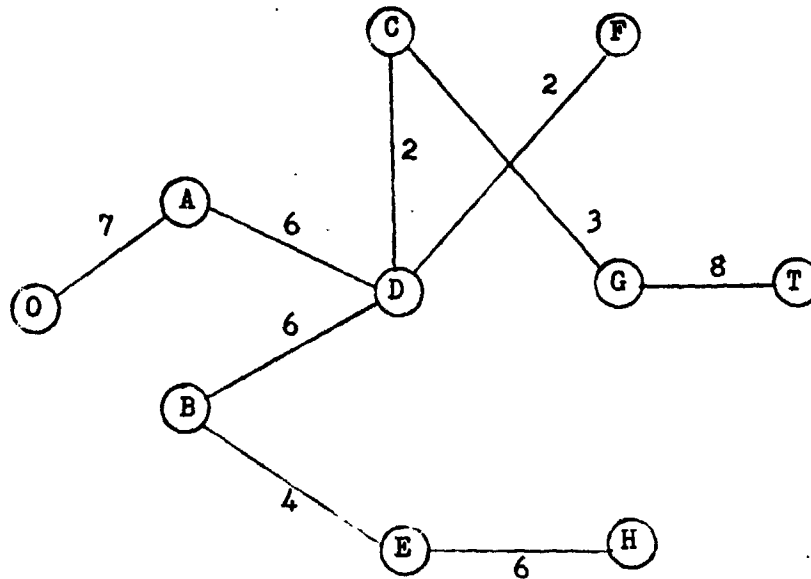
2.2.3 Minimum Spanning Tree

A variation of the Minimum Path Problem is the selection of the minimum path for a tree connecting all nodes. This tree could be used during the design of an egress system to assure the optimum placement of egress equipment relative to the work locations of personnel. As an example network, refer to the one used in this appendix in section 2.2.2. If there are some constraints to the selection of routes of egress, these should be defined at the start of the analysis. A typical constraint may be the flow capacity along each branch. Another constraint may be the degree of vulnerability of the escapees in each route relative to likely accident induced environments. To simplify the solution explanation, no constraints will be considered.

The minimal spanning tree can be determined in a straightforward manner. Beginning with any node, the first step is to pick the shortest possible branch to an adjacent node. The second step is to find the new node which is closest to either of the two connected nodes and add the appropriate branch. This process is continued until all nodes have at least one branch connecting them to the tree. The resulting network derived in this way is a minimum spanning tree. Further, the first node selected has no bearing on the resulting tree, if branch length is the only variable. If constraints must be considered, orientation or certain node pairs may need to be directly connected. In this case, it is best to add the constraints

2.2.3 (Continued)

to the network, and then solve for the minimum spanning tree in the remaining portion of the network.



EXAMPLE MINIMUM SPANNING TREE

Figure B-24

Using the example from section 2.2.2, the minimum spanning tree connecting all nodes appears as above. This represents the smallest total branch length that will connect all nodes. Had the path DC been precluded from choice by some constraint, the branch CF would have been used to connect C into the network.

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix C
FAULT TREE ANALYSIS

Contents

<u>Paragraph</u>		<u>Page</u>
	List of Figures	C-003
1.0	Fault Tree Analysis Flow	C-101
1.1	Analysis Activity	C-101
1.2	Program Activity	C-103
1.3	Fault Tree	C-104
1.4	Drawing the Tree	C-106
2.0	Fault Tree Procedure	C-201
2.1	General	C-201
2.2	Event Description	C-201
2.3	Symbols	C-202
2.4	Special Symbols	C-212
2.4.1	Matrix Gate, Introduction	C-212
2.4.2	Introduction to Advanced Concepts	C-214
2.4.2.1	Variable Type Matrix Gate	C-214
2.4.2.2	Condition Type Matrix Gate	C-217
2.4.2.3	The Matrix	C-213
2.4.2.4	Conclusion	C-221
2.4.3	Transfer Symbols	C-223
2.4.4	Output Encompassing Ellipse	C-225
2.5	Event Identification	C-225

USE FOR TYPEWRITTEN MATERIAL ONLY

<u>Paragraph</u>		<u>Page</u>
2.6	Basic Diagram Methodology	C-227
2.7	The Human Element	C-233
2.8	Dominant Paths	C-233
2.9	Fault Tree Evaluation	C-237
2.9.1	Failure Data Development for Fault Tree Evaluation	C-237
2.9.2	Fault Tree Quantitative Evaluation	C-241
2.9.2.1	Computation	C-241
2.9.2.2	Simulation	C-242
2.9.3	Constant Repair or "Lambda Tau" Method	C-243
2.9.3.1	Coexistence of Independent Failure	C-243
2.9.3.2	"AND" Gate λ	C-246
2.9.3.3	"AND" Gate γ	C-246
2.9.3.4	"OR" Gate λ	C-247
2.9.3.5	"OR" Gate γ	C-247
2.9.3.6	Failures Occuring in a Given Order	C-248
2.10	References	C-254

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix C
List of Figures

<u>Figure No.</u>		<u>Page</u>
C1	Analysis Flow	C-102
C2	Program Flow	C-105
C3	Generalized Matrix Gate	C-215
C4	Variable Matrix Gate	C-215
C5	Condition Matrix Gate	C-219
C6	Condition Matrix Gate	C-220
C7	Generalized Matrix Gate - Mathematical Equations	C-222
C8	Transfer Symbol Usage	C-224
C9	Standardized Event Notation	C-226
C10	Fault Tree Segments	C-228
C11	Fault Tree Relationships	C-231
C12	Example of Command Path	C-232
C13	Human Element Example	C-234
C14	Fault Tree Failure Data Format	C-238
C15	Lambda Tau Summary	C-253

USE FOR TYPEWRITTEN MATERIAL ONLY

1.0 FAULT TREE ANALYSIS FLOW

1.1 ANALYSIS ACTIVITY

The following problem solving steps are considered essential for a systems approach to safety. These steps will enable the risk of undesired (hazardous) events identified in the system to be maintained at an acceptable level. Starting with the System definition and information pertaining to the system configuration, then the steps are:

- 1) Identification of undesired events;
- 2) Structuring identified undesired events into a fault tree;
- 3) Determination of fault inter-relationships;
- 4) Evaluation for "likelihood" of identified undesired events;
- 5) Trade-off decisions and/or corrections.

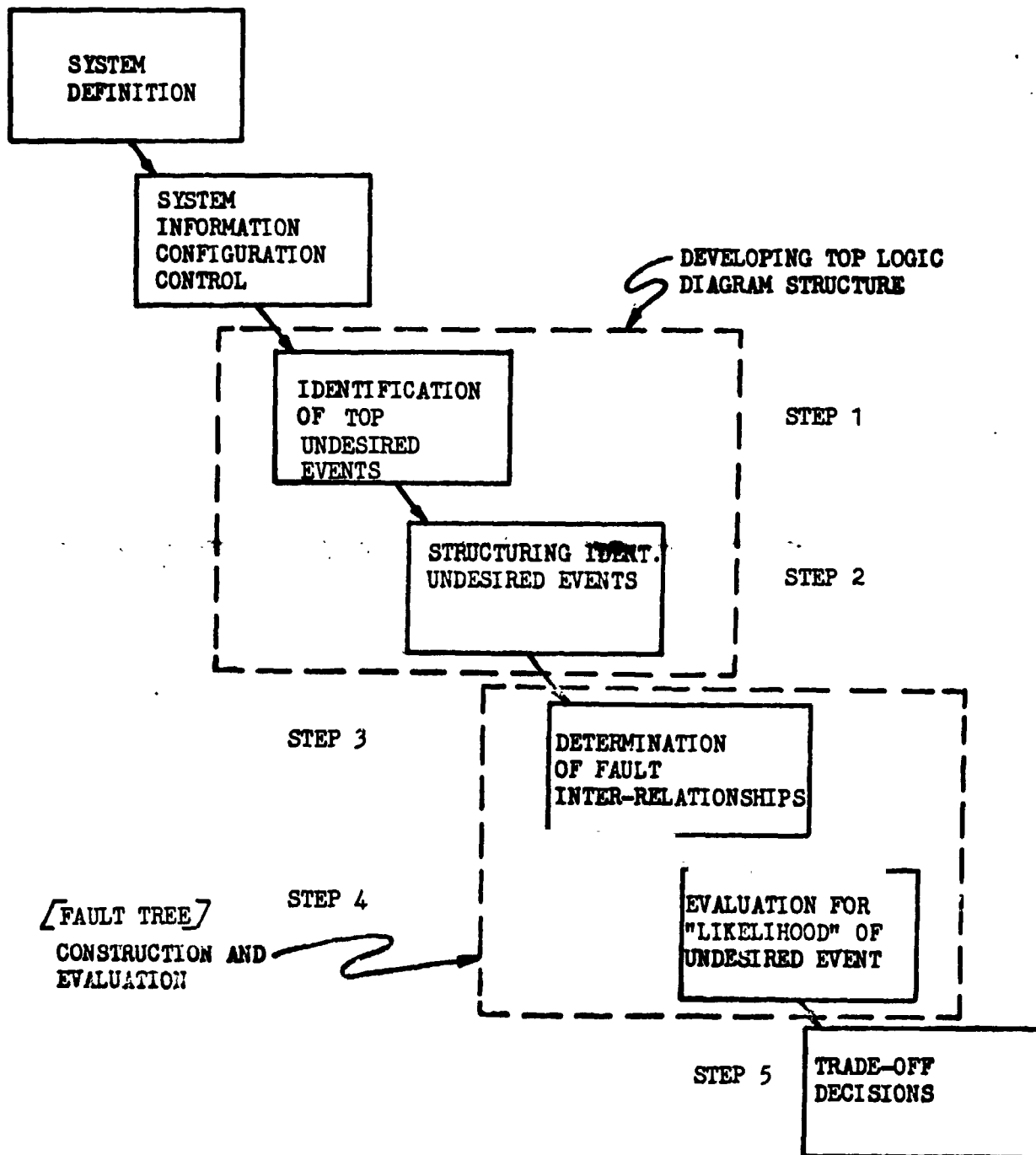
As depicted in Figure C1, steps 1) and 2) above are necessary to develop what is commonly known as a "Top" logic diagram. The top logic diagram plays an essential part in performing a system safety fault tree analysis. It is a starting guide which shows how and where the fault tree is to be developed (or expanded) by further analysis activity. It organizes all of the system unique logic relationships into a pattern whereby the system hardware and software functions can be analyzed in an orderly and logical manner. This means that the top must be structured so that the end analysis is complete in satisfying what is defined by the top undesired event(s).

System unique logic relationship variables which must be carefully structured are things such as: a) system operation modes, b) mission phases and/or operations, c) the degree of man/machine relationship in the system, d) inter-relationships of the Centers with the system functions, and e) functional order of the system.

This list of relationship variables covers the top structure gross considerations, and indicates the types of activity involved. The system unique logic relationship variables will vary with the different systems being analyzed, with the degree of difference depending upon the similarity between systems.

As already stated, the top logic diagram is a starting "guide" for a complete system fault tree analysis. This means that once the top is started it is not necessarily "cast in concrete", but is subject to change as analysis activity progresses. Experience has shown that as an analysis proceeds to completion, more system information and understanding is gained. As system information and understanding develop, modification to the top logic diagram is required to reflect this current knowledge.

USE FOR TYPEWRITTEN MATERIAL ONLY



ANALYSIS FLOW

FIGURE C -1

SHEET C-102

1.1 (Continued)

Step 3) is the actual development of the logic diagram. This is the point where analysis activity proceeds from the top logic diagram structure and continues through the hardware level. This step is the foundation of a fault tree analysis. The fault mode relationships, once correctly and completely structured, will usually never change - unless hardware design changes occur.

Step 4) is an evaluation of the completed fault tree for the purpose of: a) determining the likelihood of identified events, and b) determining the identity and ranking of "chains" of events and event relationships leading to the identified undesired event(s). Evaluation can be accomplished by rigorous mathematical processes (quantitative evaluation) or from intuitive (inductive) methods. However, the results obtained (quantitative/inductive) will only be as complete as the applied rigor. Useful results can be obtained from evaluations made during the course of development of the fault tree analysis.

Should a quantitative evaluation be required, an equation can be written for the entire fault tree. By use of Boolean algebra, Lambda Tau methods or Monte Carlo methods the equation can be simplified and solved to give a meaningful solution. Except for very small trees, the use of a computer is required. See the list of references for sources of information on employing these mathematical solutions.

Step 5) If it is determined through the evaluation of the fault tree (or as a result of other analyses) that corrective action is required, the fault tree analysis itself is a valuable source of information for change decisions. Proposed corrections such as design changes, procedure changes, etc., can be evaluated in the context of the fault tree to determine a relative measure of improvement.

In order to achieve a meaningful and useful analysis, two important points must be emphasized. First, the output of an analysis is only as valuable and reliable as the quality and quantity of effort and information going into the analysis. Second, hardware and operating procedures configuration control must be maintained at all times to avoid erroneous conclusions being drawn from the analysis.

1.2 PROGRAM ACTIVITY

The Fault Tree technique can be used to perform a complete system-integrated analysis, or for a small problem containing less than ten events. In any case the flow sequence of analysis will follow the outline to some degree as described below.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.2 (Continued)

The flow of activity necessary for a complete system-integrated fault tree analysis should follow a pattern as shown in Figure C2. This flow takes into consideration the steps required to perform an analysis, along with the difficult task of consolidating the event analyses into one complete system/mission oriented analysis.

As shown in Figure C2, the first step in the analysis program development is the structuring of the top logic diagram. After a suitable top has been structured and agreed upon by all involved, each of the analysts is assigned specified portions of the fault tree for further development. While the analyses are being conducted, the task of reviewing the output of each analysis and combining the output into one complete systems analysis is performed by those who developed the top diagram. When the analysis for system safety is complete, it will be documented.

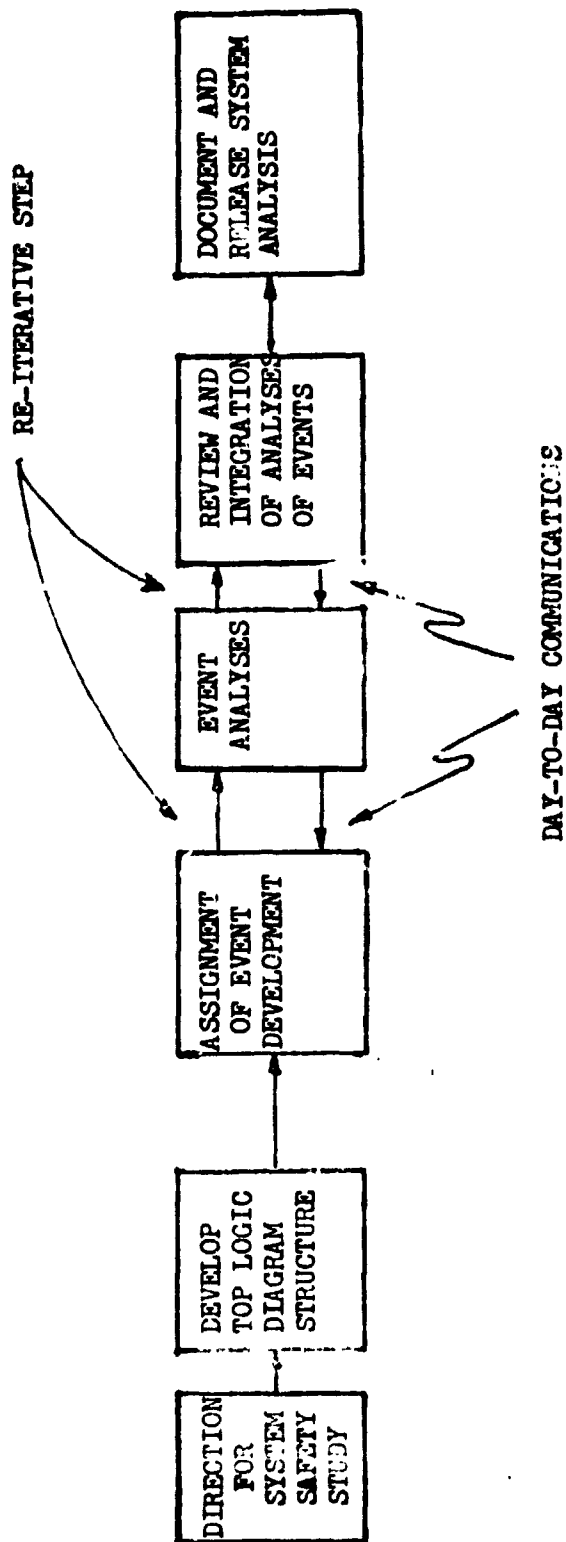
An important factor necessary in accomplishing a system-integrated analysis is effective communications on a "day-to-day" basis between all the analysts involved.

1.3 FAULT TREE

The following guidelines may be used to achieve a consistency of approach and to assure analysis completeness.

- 1) Structuring should follow the rules and symbolism used in this appendix, since they are well standardized throughout the aerospace industry.
- 2) Each "diamond" event should have the following information and reason for analysis termination of the event:
 - (a) Insignificant (with rationale), or
 - (b) Lack of system information, or
 - (c) Identification of other analyses which satisfactorily analyze the failure modes and system effects for that event.
- 3) Development information sources should be identified by schematic, flow, time, mechanical, electrical, operation, maintenance drawing and/or document numbers. The revision date and/or number must be included for each source. This source information must be included as part of each submittal.

USE FOR TYPEWRITTEN MATERIAL ONLY



PROGRAM FLOW

FIGURE C2

1.3 (Continued)

- 4) Each analyst must utilize the fault tree alphabetic code assignments made in the computer drawing program, if one is being used.
- 5) Revision codes should be included by each analyst and can be based on the standard practice of assigning progressive alphabetic characters beginning with A.
- 6) Identify all components and subsystems by part number.

1.4 Drawing the Tree

In some cases, the analysts may make hand sketched trees, and document the evaluation and conclusions. In other cases, where more complicated trees are involved, and presentations to substantiate the conclusions must be made to management, then formal drafted trees may be prepared. Where complicated integrated systems are being analyzed, there are computer controlled drafting systems available. See the list of references for sources of information on these systems.

USE FOR TYPE-SET MATERIAL ONLY

2.0 FAULT TREE PROCEDURE

2.1 GENERAL

A fault tree is a diagram of the logical relationships of parallel and series combinations of independent personnel or equipment subsystem and component failures and normal operating modes that can result in a specified undesired event. This diagram can be quantified to provide a relative probability of causing the specified undesired event by means of each path leading to that event. Paths having high relative probability are considered dominant over paths of low probability.

The following sections discuss basic rules, definitions and methods of the fault tree technique.

2.2 EVENT DESCRIPTION

The term "event" denotes a dynamic change of state that occurs to a system element, where an element is inclusive of hardware, software, personnel and environment. If the change of state is such that the intended function of the particular element is not achieved, or an unintended function is achieved, the event is an abnormal system function or "fault event." If the change of state is such that the intended function occurs as planned (designed), the event is then a normal system function or "normal event." Thus, two types of events exist -- those which are not intended and those which are intended.

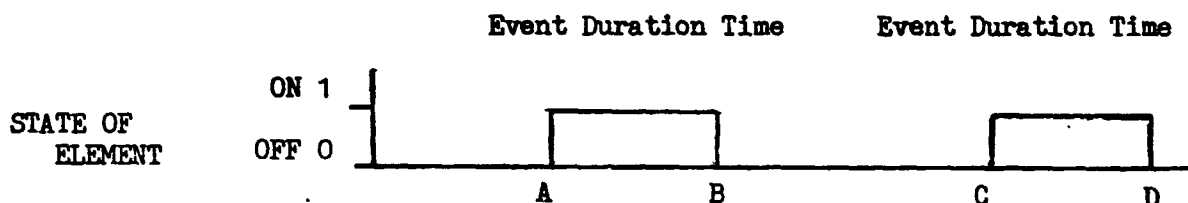
Fault events can be divided into two categories: basic events and gate events. Basic events are events whereby system elements (usually at the component level) go from an unfailed state to a failed state, and are related to a specific failure rate and fault duration time. These events are used only as inputs to a logic gate (never as outputs) and are therefore independent events. On a fault tree, basic events are depicted by a circle or a diamond. A gate event is the event (or system failure) which results from the output of a logic gate. Since the gate event is dependent upon the input events and the type of logic gate function, it is therefore a dependent event. It must be noted that the gate event is not the logic gate itself, but the result of the logic gate function and the input events. The gate event is depicted by a rectangle above the logic gate. As fault tree development progresses, gate events on one level become inputs to gate events on the next higher level. (See Section 2.3 for examples.)

In the fault tree analysis of a system the inherent modes of failure of system elements are delineated as primary, secondary and command. These failure modes are referred to as "primary events," "secondary events," and "command events" respectively, and are depicted on the fault tree as the combination of basic events and/or gate events. In other words, these events are generally identified at a gate event level, and depending on the level of analysis, are further developed until the event can be identified in terms of basic events.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.2 (Continued)

In a fault tree analysis, the dynamic change of state that occurs to a system element is defined as a binary type event. That is, a system element is always in one of two states, ON or OFF. The ON state (or 1) corresponds to a failed condition and the OFF state (or 0) corresponds to an unfailed condition. The example below illustrates the binary manner of a system element. The element operates normally (OFF state) until failure occurs (ON state). After the fault event occurs (dynamic change of state) the element remains failed (ON state) until repair of some sort has been effected. When repair is accomplished, the element returns to the unfailed state (OFF). By representing events and gates in a binary manner, fault trees can be analyzed by the rigorous techniques of Boolean algebra.



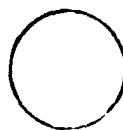
- A - Time of 1st failure
- B - Time 1st failure is repaired
- C - Time of 2nd failure
- D - Time 2nd failure is repaired

2.3 SYMBOLSRectangle

The rectangle identifies an event (gate event) that results from the combination of fault events through a logic gate. The rectangle is also used to describe a conditional input to a functional condition INHIBIT gate (described below).

Circle

The circle describes a basic fault event that requires no further development. The frequency and mode of failure of items so identified is derived from empirical data. The rate of occurrence of such a primary event is normally the generic failure rate of the component for the particular failure mode.



USE FOR TYPEWRITTEN MATERIAL ONLY

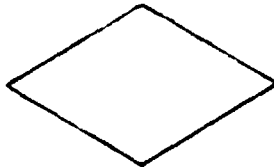
2.3 (Continued)

House

The house indicates an event that must occur (or is expected to occur) due to normal operating conditions in the system. The house does not indicate a fault event. An example is a phase change in a dynamic system, such as the landing, flight, and take-off phases of an aircraft.

Diamond

The diamond describes a fault event that is considered basic in a given fault tree. The possible causes of the event are not developed either because the event is of insufficient consequence or the necessary information for further development is unavailable. It also can indicate non-development because an analysis already exists that is of satisfactory depth and breadth. Which of the three uses that applies, should be indicated for each diamond on the tree.

Oval

The oval is used to record the conditional input to a random condition INHIBIT gate. It defines the state of the system that permits a fault sequence to occur, and may be either normal to the system or result from failures. It is also used to indicate the necessary sequence of events required to pass through an "AND" or an "OR" gate function.

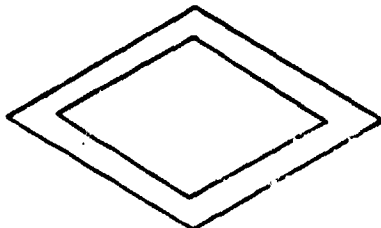


USE FOR TYPEWRITTEN MATERIAL ONLY

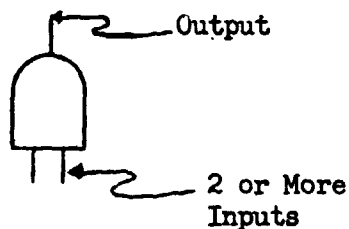
2.3 (Continued)

Double Diamond

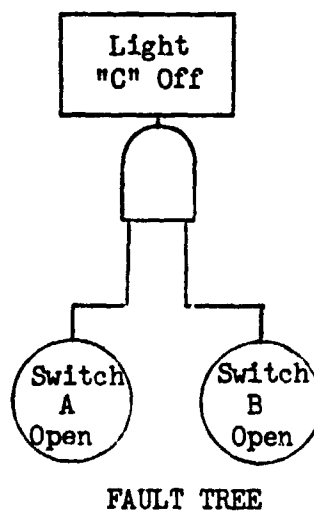
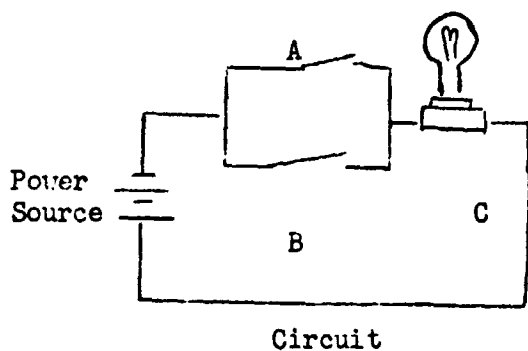
The double diamond is used in the simplification of a fault tree for numerical evaluation. The event described results from the causes that have been identified, but are not shown on a particular version of the fault tree being examined.

"AND" Gate

The "AND" gate describes the logical operation whereby the co-existence of all input events is required to produce the output event. The fault duration time of an "AND" gate is expressed in terms of the input fault duration times.

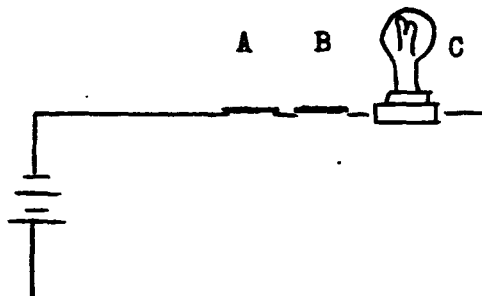


Example of "AND" Gate Usage:

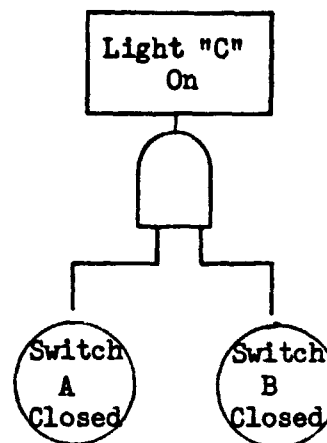


2.3 (Continued)

Another example of "AND" Gate Usage:



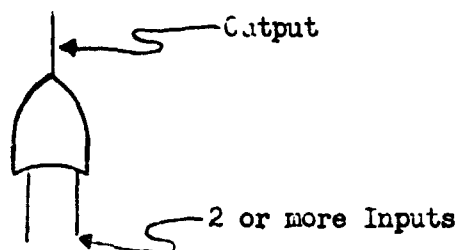
Circuit



FAULT TREE

"OR" Gate

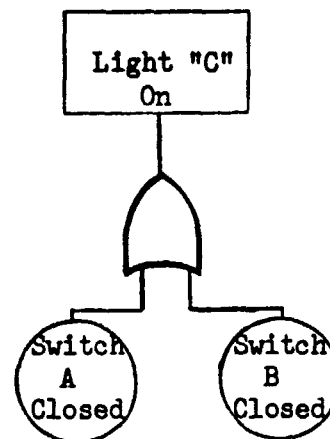
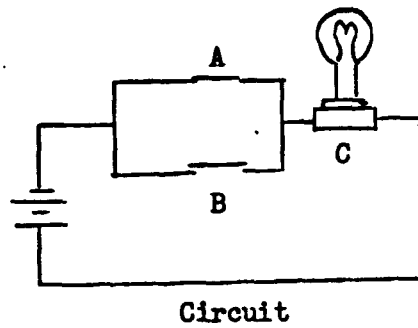
The "OR" gate defines the situation whereby the output event will exist if one or more of the input events exists. The fault duration time of an "OR" gate is expressed in terms of the input fault duration times.



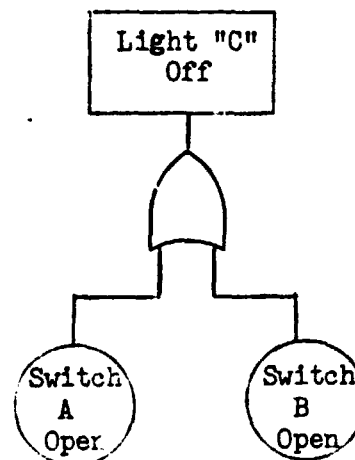
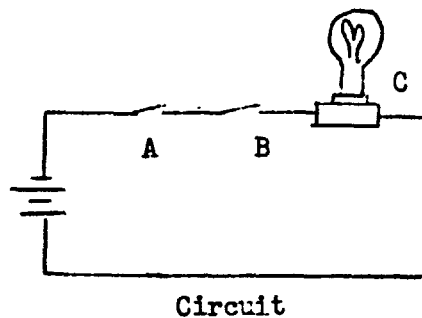
USE FOR TYPEWRITTEN MATERIAL ONLY

2.3 (Continued)

Example of "OR" Gate Usage:



Another example of "OR" Gate Usage:

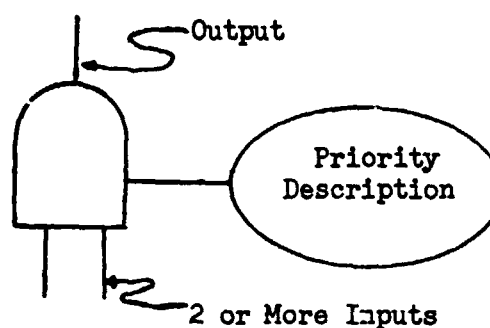


USE FOR TYPEWRITTEN MATERIAL ONLY

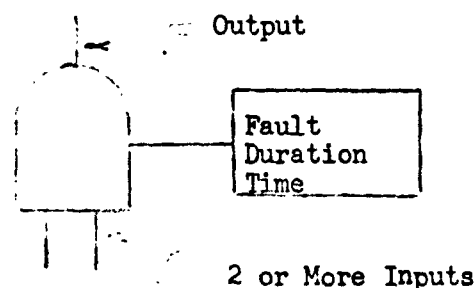
2.3 (Continued)

"PRIORITY AND" Gate

The "PRIORITY AND" gate performs the same logic function as the "AND" gate with the additional stipulation that sequence as well as co-existence is required.

"CONSTANT FAULT DURATION AND" Gate

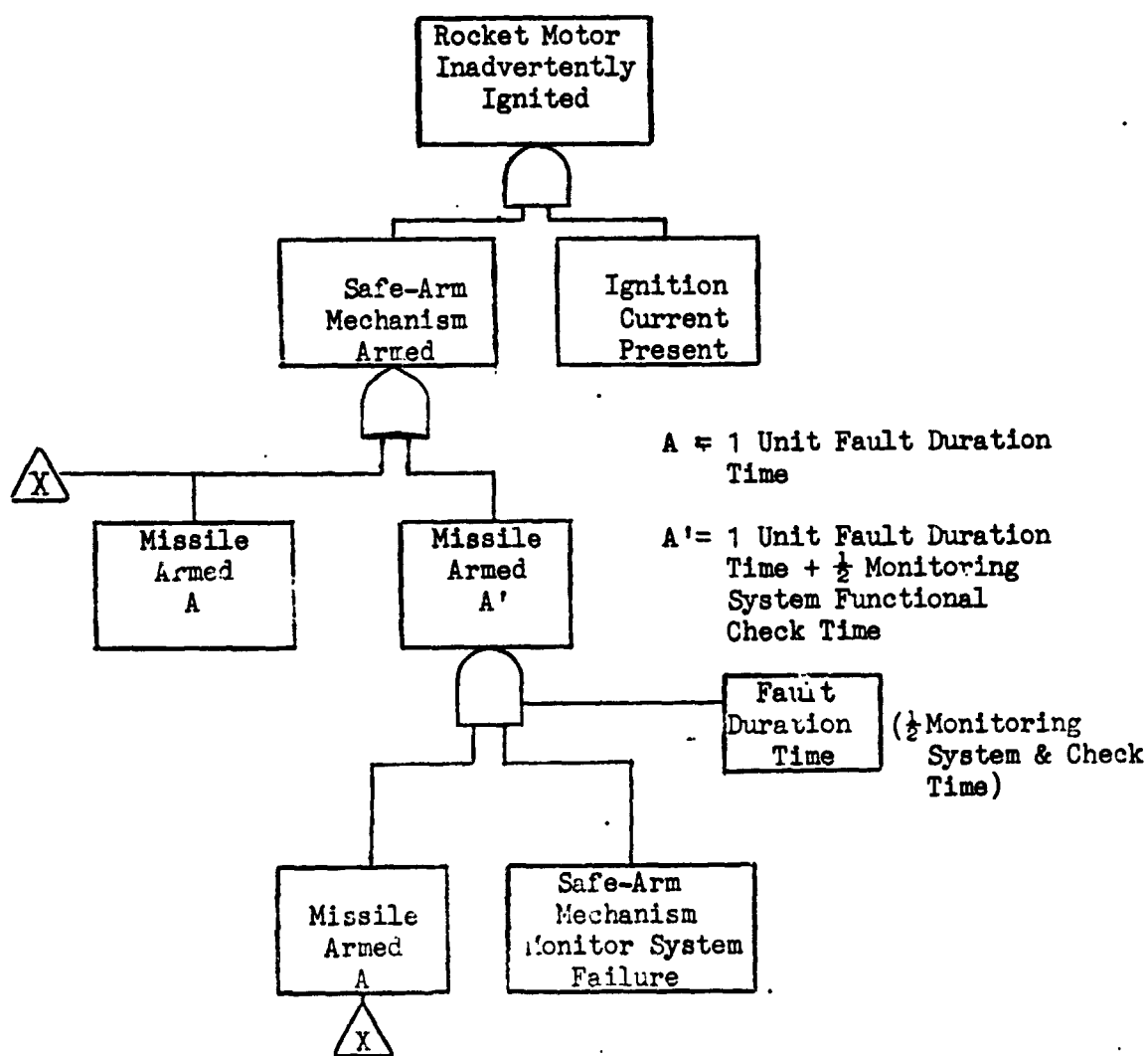
The "CONSTANT FAULT DURATION AND" gate symbolized describes the same logical function as the "AND" gate except that the fault duration time of the output event is not dependent upon the fault duration times of the inputs. The fault duration time of this gate is determined as a function of the system operation.



2.3 (Continued)

Example of "CONSTANT FAULT DURATION AND" Gate Usages

Consider the undesired event "Rocket Motor Inadvertently Ignited." Assume the "armed" results in a warning light prompting immediate repair action. If the "armed" event occurs and the warning system is working, the fault duration time is one unit. If the "armed" event occurs and the warning system has failed, the fault duration time is naturally longer, being dependent upon how often the monitoring system is functionally checked.

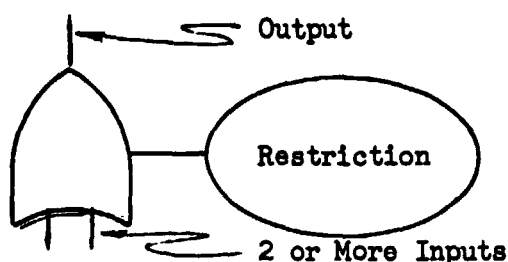


FAULT TREES

2.3 (Continued)

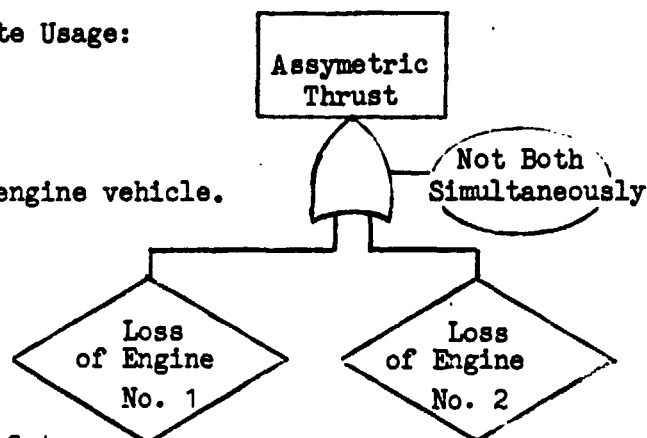
"EXCLUSIVE OR" Gate

The "EXCLUSIVE OR" gate functions as an OR gate with the restriction that specified inputs cannot co-exist. This gate will not respond to the co-existence of Two or more specified input events.

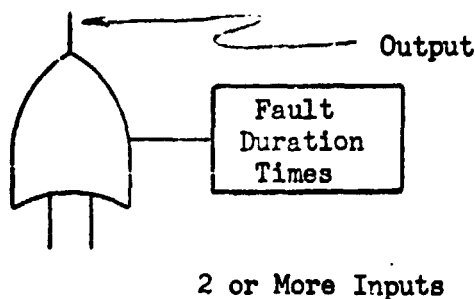


Example of "EXCLUSIVE OR" Gate Usage:

Assume: Twin, side mounted engine vehicle.

"CONSTANT FAULT DURATION OR" Gate

The "CONSTANT FAULT DURATION OR" gate performs the same function as the "OR" gate except that the fault duration time of the output event is not dependent upon the fault duration times of the inputs. The fault duration time of the output event is strictly dependent upon system operation variables, and must be determined from system information rather than in terms of the input event fault duration times.

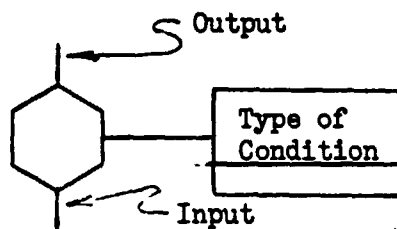


USE FOR TYPEWRITTEN MATERIAL ONLY

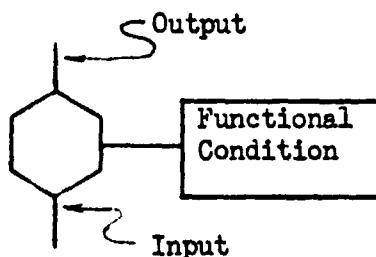
2.3 (Continued)

"INHIBIT" Gates

"INHIBIT" gates describe a causal relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied. The conditional input defines a state of the system that permits the fault sequence to occur, and may be either normal to the system or result from failures. The conditional input is represented by an oval if it describes a specific failure mode and a rectangle if it describes a condition that may exist for the life of the system. The conditional input is further described on the following pages. The logical "INHIBIT" functions are symbolized in fault trees as follows:

"FUNCTIONAL CONDITION INHIBIT" Gate

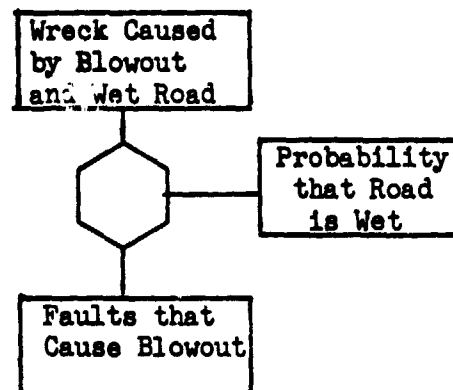
The "FUNCTIONAL CONDITION INHIBIT" gate provides a means for applying conditional probabilities to the fault sequences. If the input event occurs and the "condition" is satisfied, an output event will be generated. The duration time of the output event may be either the duration time of the fault input or may be separately generated.



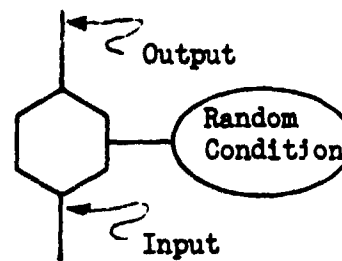
USE FOR TYPEWRITTEN MATERIAL ONLY

2.3 (Continued)

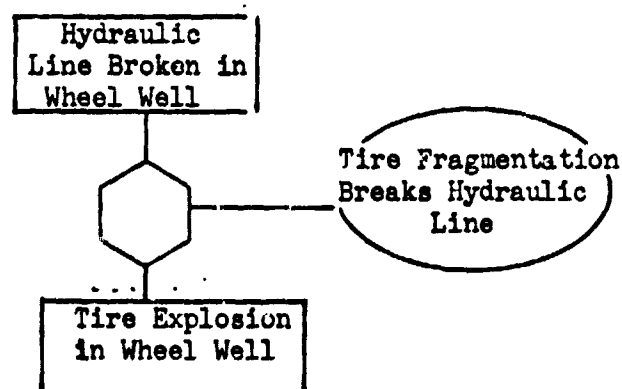
Example of "FUNCTIONAL CONDITION INHIBIT" Gate Usage:

"RANDOM CONDITION INHIBIT" Gate

The "RANDOM CONDITION INHIBIT" gate is the same as the "FUNCTIONAL CONDITION INHIBIT" gate except that the status of the conditional input to a "RANDOM CONDITION INHIBIT" gate is variable while it remains constant in the "FUNCTIONAL CONDITION INHIBIT" gate. The fault duration time of the output event is always generated within the gate.



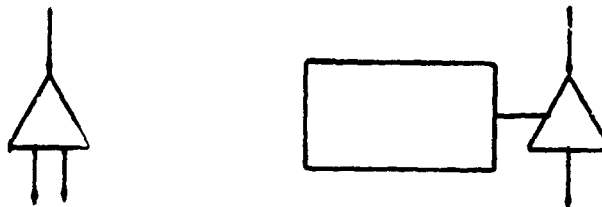
Example of "RANDOM INHIBIT" Gate Usage:



2.4 SPECIAL SYMBOLS

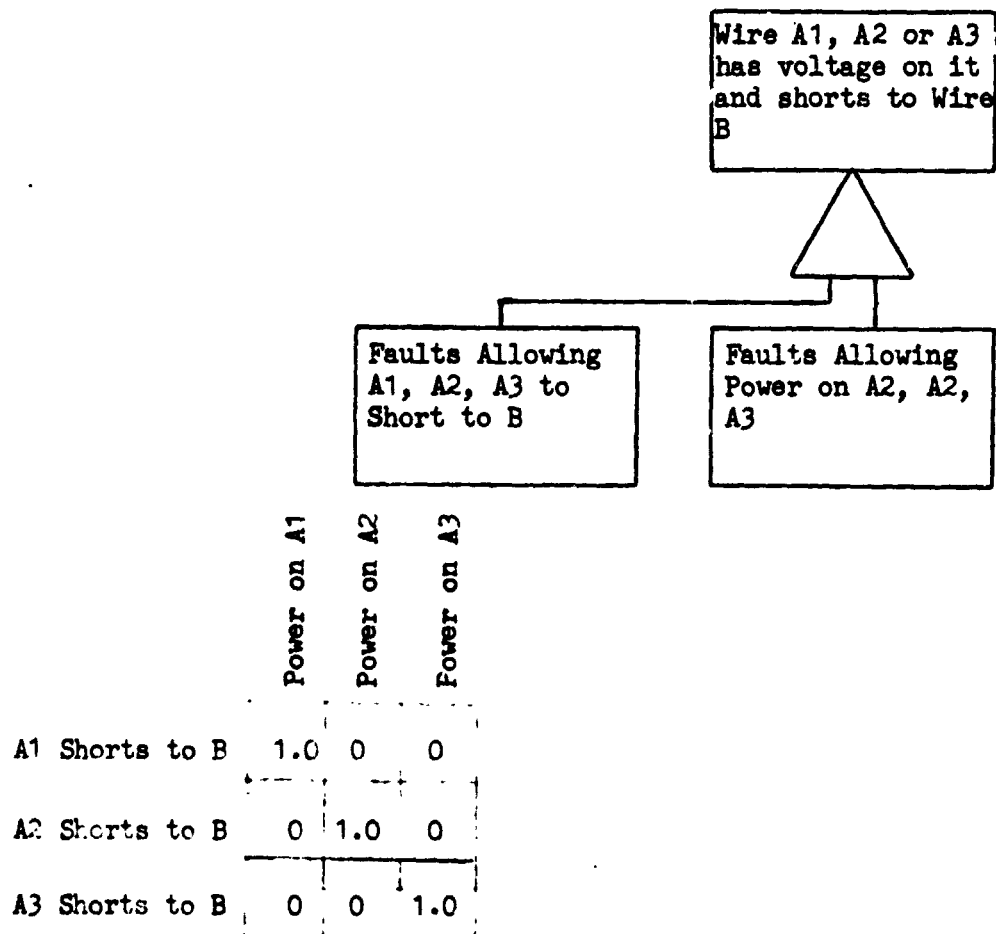
2.4.1 "MATRIX" Gate, Introduction

Variable Type



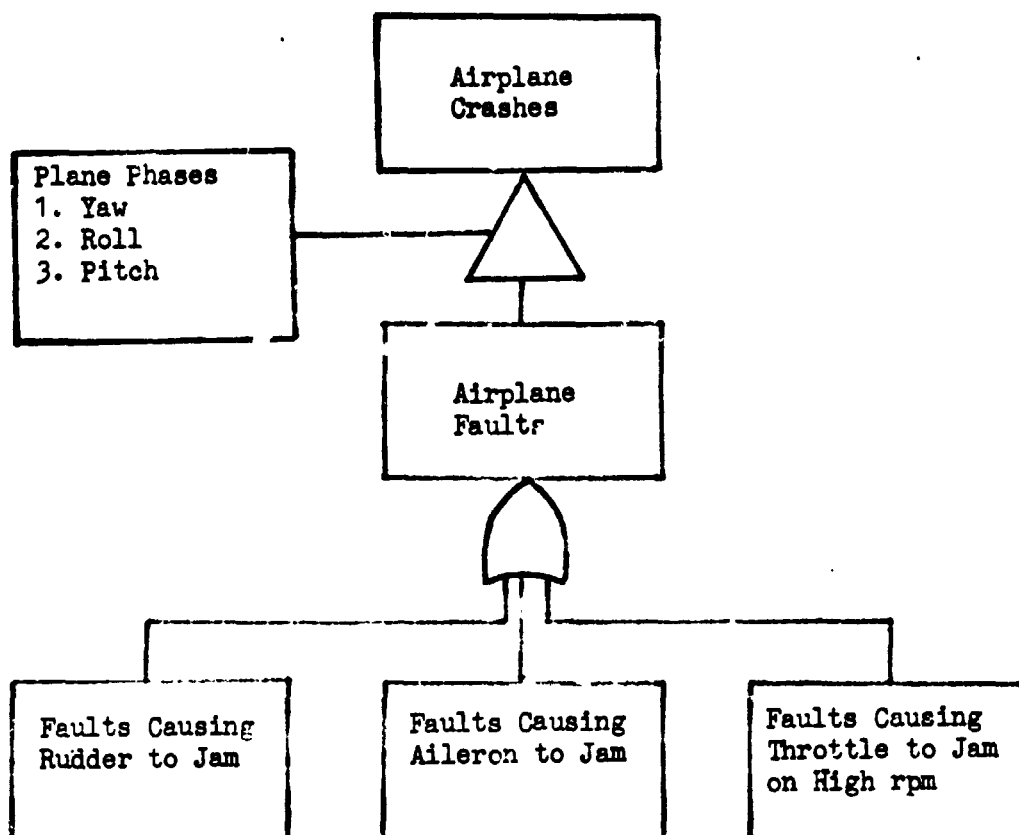
The "MATRIX" gate is used to describe a situation in which an output event is produced for certain combinations of events at the inputs. A matrix showing the event combinations that produce the output event accompanies each usage of this symbol.

Example of "VARIABLE TYPE MATRIX" Gate Usage



USE FOR TYPEWRITTEN MATERIAL ONLY

"CONDITIONAL MATRIX" Example



USE FOR TYPEWRITTEN MATERIAL ONLY

	Rudder Jams	Aileron Jams	Throttle Jams on High rpm
Roll	.4	.5	.3
Pitch	.7	.8	.4
Yaw	.6	.7	.6

2.4.2 Introduction to Advanced Concepts in the Usage of the Matrix Gate

In fault tree analysis of systems and subsystems many fault events are used repeatedly in order to denote the proper sequence of logic leading to an undesired event. Frequently the redundant fault events are related to one another by a second fault event, resulting in a unique combination of events. When these combinations are expressed by conventional fault tree techniques, the result is usually long and repetitive. The Matrix Gate is a method by which fault tree diagram construction is simplified with reference to permutations of redundant (or similar) fault events.

It must be emphasized that the Matrix Gate is not a unique logic operator in fault tree analysis techniques. The Matrix Gate is merely a simplified or abbreviated representation of an already existing portion of a fault tree; the existing portion of a fault tree being a series of two-input AND gates (with related inputs) summed together by an OR gate.

Whenever the Matrix Gate is used it is accompanied by a matrix, whose elements are the redundant (or similar) fault events. This matrix is necessary in order to denote which combination of events are applicable to the analysis, the total number of combinations, and the probability of a particular combination resulting in the undesired event.

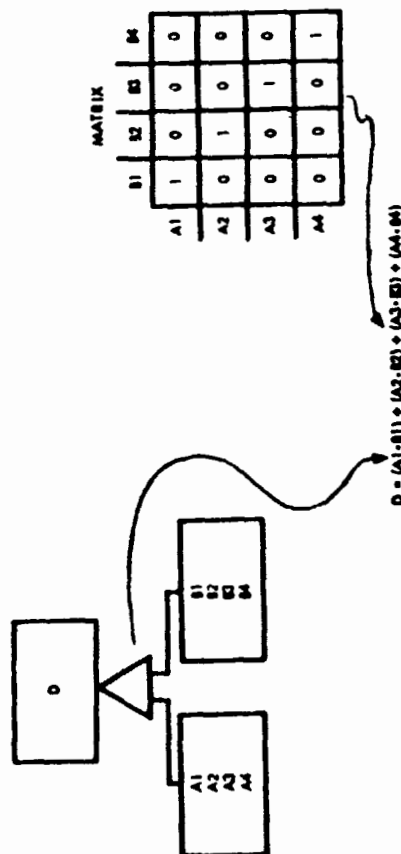
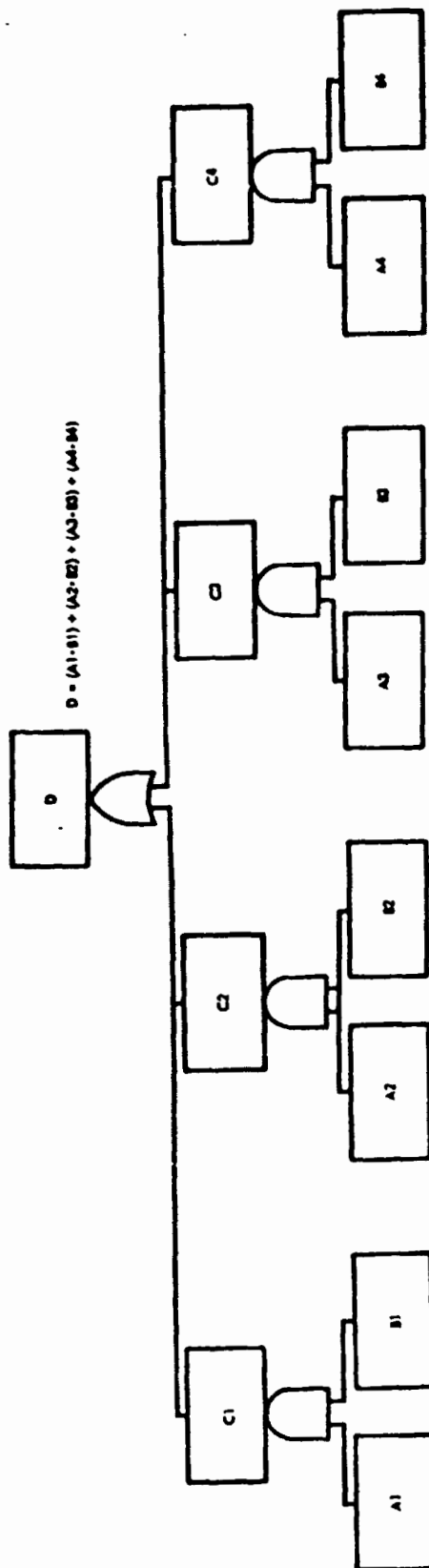
In order for the Matrix Gate to meet all possible situations it is necessary for two types of gate to exist; the variable type Matrix Gate and the conditional type Matrix Gate. The variable type gate handles situations where both of the inputs to the gate consist of fault events (fault events being referred to as variables). The conditional type gate handles situations where one input consists of fault events (variable) and the other input consists of conditional events.

Example 1 (Figure C3) is a generalized case using the variable type Matrix Gate. Fault events A1, A2, A3 and A4 are unique but similar and fault events B1, B2, B3 and B4 are unique but similar. The Boolean Expression derived from the sample fault tree agrees with the Boolean expression extracted from the Matrix Gate and its associated matrix.

2.4.2.1 Variable Type Matrix Gate

Example 2 (Figure C4) is a typical problem in which a four-wire cable is to be analyzed. The wires are identified as A1, A2, A3 and B. Under standby operating conditions, assume that none of these wires carry voltage, and furthermore, that wire B is an ordnance line and wires A1, A2 and A3 carry voltage at certain discrete time intervals. The undesired event is wire A1, A2, or A3 shorting to wire B and at the same time having voltage on it from a fault condition at the voltage source.

USE FOR TYPEWRITTEN MATERIAL ONLY



MATRIX

	B1	B2	B3	B4
A1	1	0	0	0
A2	0	1	0	0
A3	0	0	1	0
A4	0	0	0	1

Example 1

Figure C3
Generalized Matrix Gate

Example 2

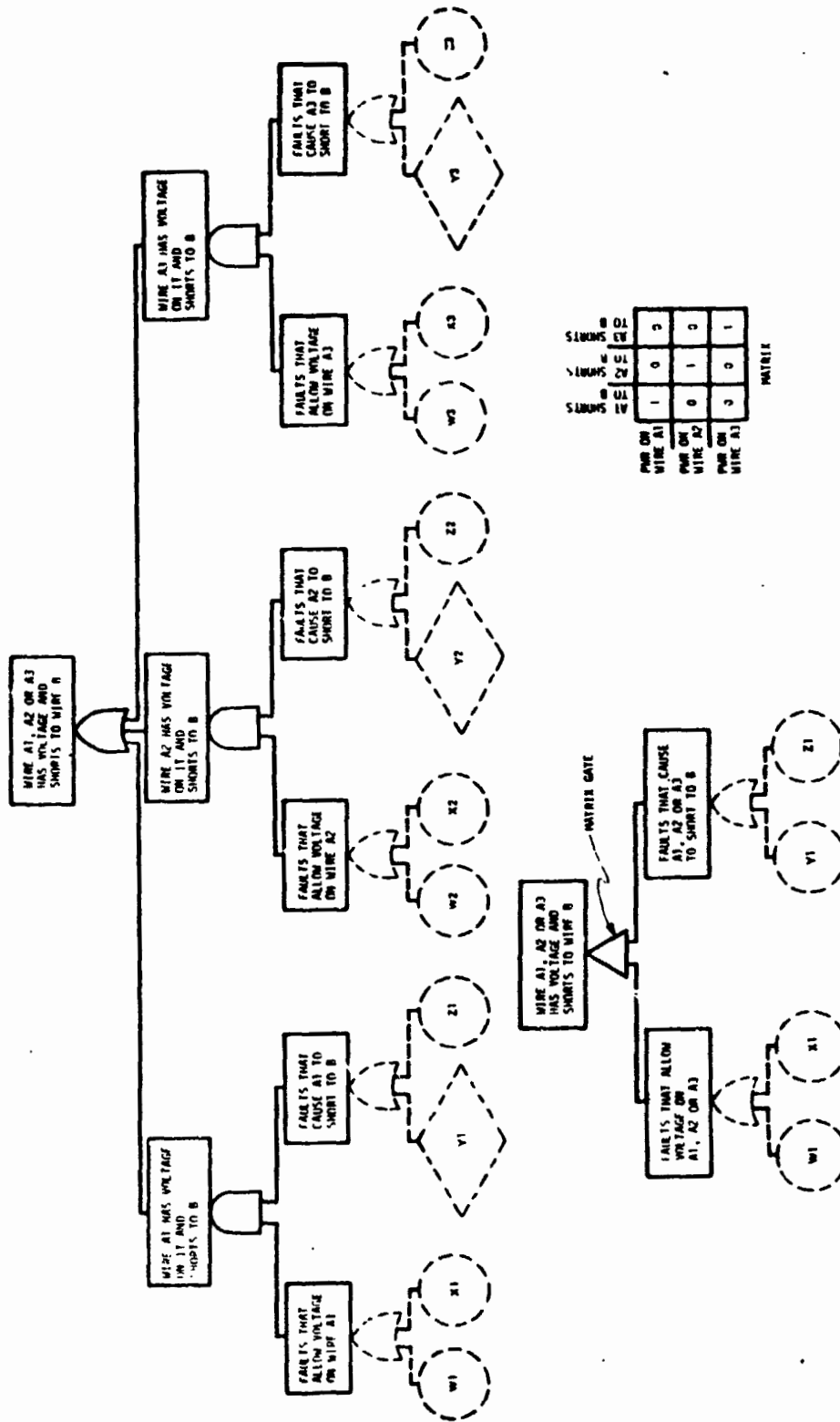


Figure C4
Variable Matrix Gate

2.4.2.1 (Continued)

In this example the events which cause wire A1 to short to wire B will be similar to the events which cause wire A2 to short to wire B and wire A3 to short to wire B. For example, they could be shorts caused by an insulation failure or a primary wire failure. Therefore, the fault conditions of these three wires are unique, yet similar. Since they are similar, they are drawn only once with the Matrix Gate, instead of three times under conventional techniques.

The fault events which allow power onto wire A1 may or may not be similar to the events which allow power onto wire A2 or A3, depending upon the circuitry involved. If the fault events are similar (or the same) the Matrix Gate can be utilized easily, with the fault event drawn only once. However, if the fault events are completely different for each wire, the Matrix Gate becomes more complex, and each distinct fault event must be drawn (with little saving over conventional techniques). Since the circuitry at the voltage source is not developed in this example, an assumption will be made that the faults are similar for each wire.

The 3 x 3 matrix drawn in Example 2 points out the combinations of interest in this particular analysis. The boxes which contain a "one" are the combinations of concern. These boxes, figuratively speaking, say that "the faults allowing power on wire A1" are ANDED with "the faults causing wire A1 to short to wire B", and "the faults allowing power on wire A2" are ANDED with "the faults causing wire A2 to short to wire B", and "the faults allowing power on wire A3" are ANDED with "the faults causing wire A3 to short to wire B" which are all summed together by an OR gate.

The significance of using a Matrix Gate in Example 2 may not be readily apparent, but suppose the four-wire cable had been a 50 wire cable. Instead of drawing 50 iterations of wire shorts combined with faults allowing power on the wire, the Matrix Gate requires only one iteration of the combination. The tediousness of drawing and reading superfluous information has been eliminated, yet the necessary information is not lost.

2.4.2.2 Condition Type Matrix Gate

Example 2 demonstrated the Matrix Gate with both of the inputs as variables. That is, both of the inputs to the gate consisted of fault conditions. A second, and slightly different, way of using the Matrix Gate is with one input as a variable and the other input as a condition. This type of usage is fitted for situations whereby the Matrix Gate is employed to replace Inhibit Gates which have similar or redundant inputs. Example 3 depicts this type of usage.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.4.2.2 (Continued)

Example 3 (Figure C5) deals with a car and highway situation. In this example a car is analyzed for the undesired event "car wreck" and the only failure modes being considered are: 1) blowout, 2) loss of steering, and 3) brakes locking. In addition to analyzing the car to determine the causes of these failure modes, certain road conditions are placed on each failure mode. These conditions are: 1) the road being wet, 2) the road being dry, and 3) the road being icy.

As is apparent from the fault tree shown in Example 3, the variable inputs to the Inhibit Gates are redundant, and result in a unique set of combinations. This unique set of combinations results in a long and repetitious fault tree, which can be effectively reduced in size and complexity as shown.

The 3 x 3 matrix shown in Example 3 demonstrates that nine unique, but related combinations result from this particular example. Furthermore, it shows which fault event is combined with which conditional event, and the number of times each event is combined.

2.4.2.3 The Matrix

Now that the Matrix Gate has been exemplified in a simple and concise manner, a small adjustment factor must be introduced. This adjustment factor involves the "one" and "zero" placed inside the boxes of the matrices. These numbers are in actuality probability numbers which represent the probability of an Inhibit Gate allowing each combination (of fault events) to result in the undesired event. To be specific, an Inhibit Gate is located between each AND gate combination and the summing OR Gate. This "hidden" Inhibit Gate does not appear in the fault trees of Examples 1, 2, and 3 because the probability of a particular combination resulting in the undesired event has been assumed as one or zero. When the probability was zero for a certain combination this meant that the combination was either impossible or not desired for analysis. When the probability was one for a certain combination this meant that when the two events occurred, the undesired event was immediately realized. The probability of the combination resulting in the end event is not always one or zero, but frequently some value in-between.

Example 4 (Figure C6) is a continuation of Example 3, except the "hidden" Inhibit Gate is shown in the diagram. This example demonstrates the probability involved for realizing a car wreck given that a car fault occurs and the appropriate road condition is fulfilled. Take for example the fault tree path "blowout on a wet road". When a blowout occurs and the road is wet it does not necessarily follow that there will be a car wreck. There is a certain probability involved for a blowout on a wet road to result in a wreck, and this probability is represented by an Inhibit Gate condition. The probability of this condition is placed inside the matrix which accompanies the Matrix Gate.

USE FOR TYPEWRITTEN MATERIAL ONLY

Example 3

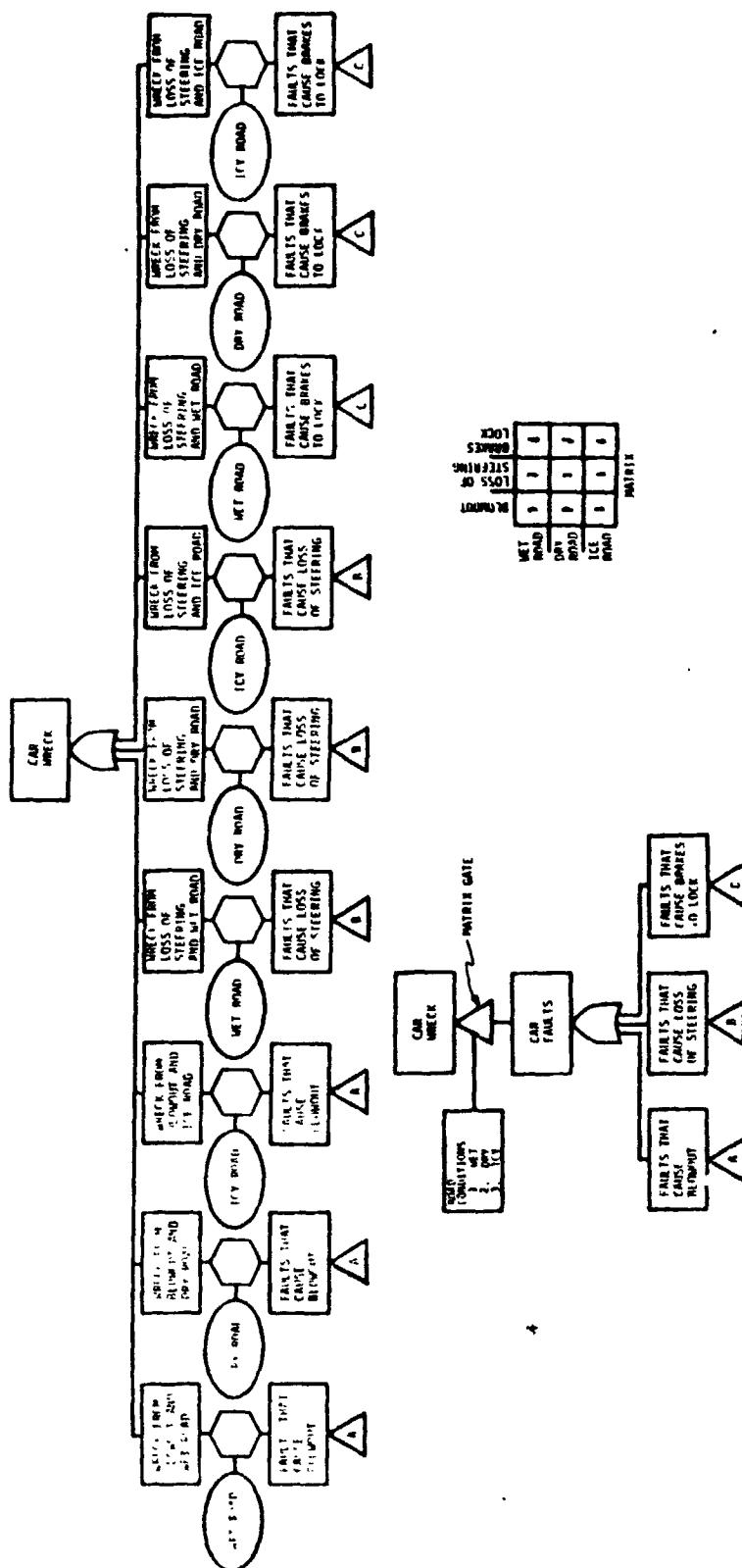
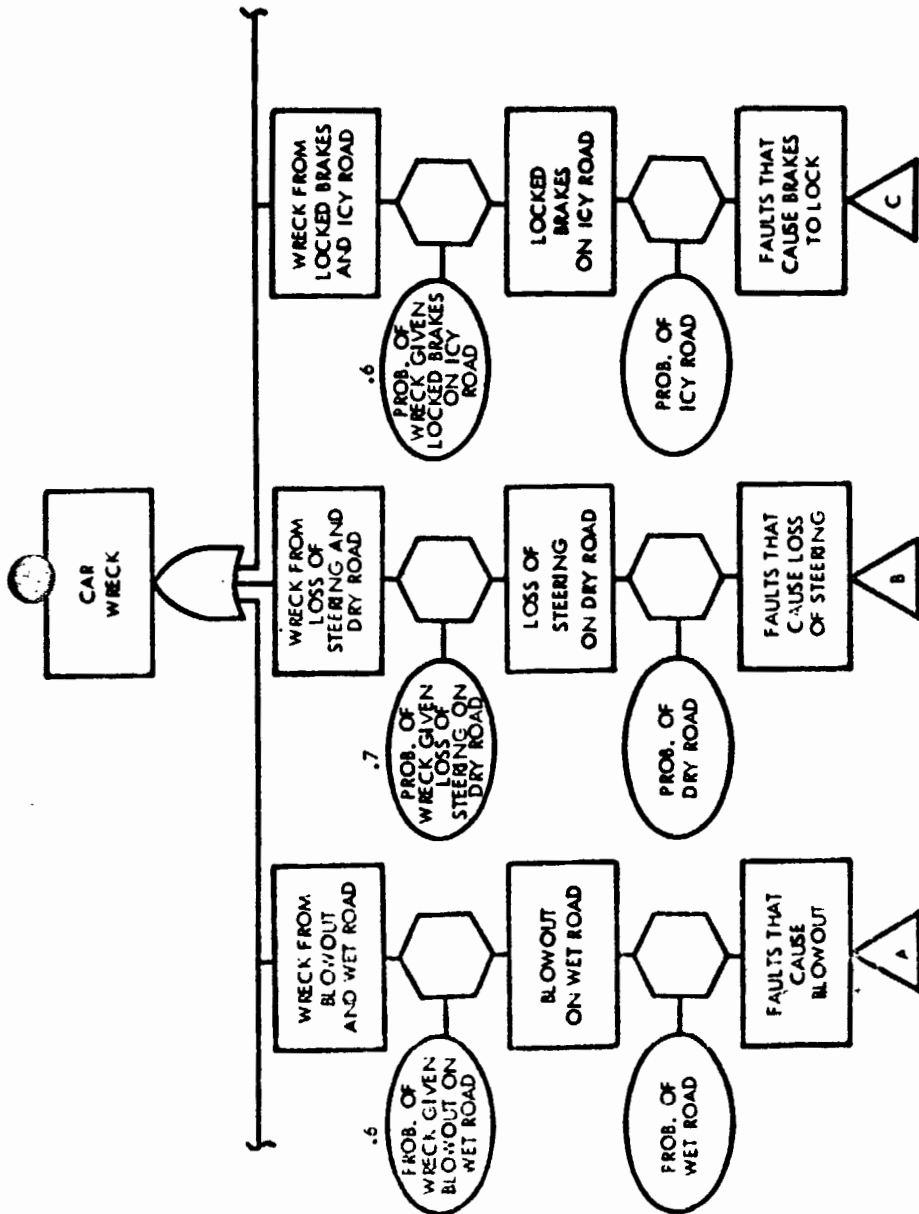


Figure C5
Condition Matrix Gate

Example 4



	BLOWOUT	LOSS OF STEERING	BRAKES LOCK
WET ROAD	.6	.8	.5
DRY ROAD	.4	.7	.4
ICY ROAD	.5	.9	.6

MATRIX

Figure C.6
Condition Matrix Gate

2.4.2.3 (Continued)

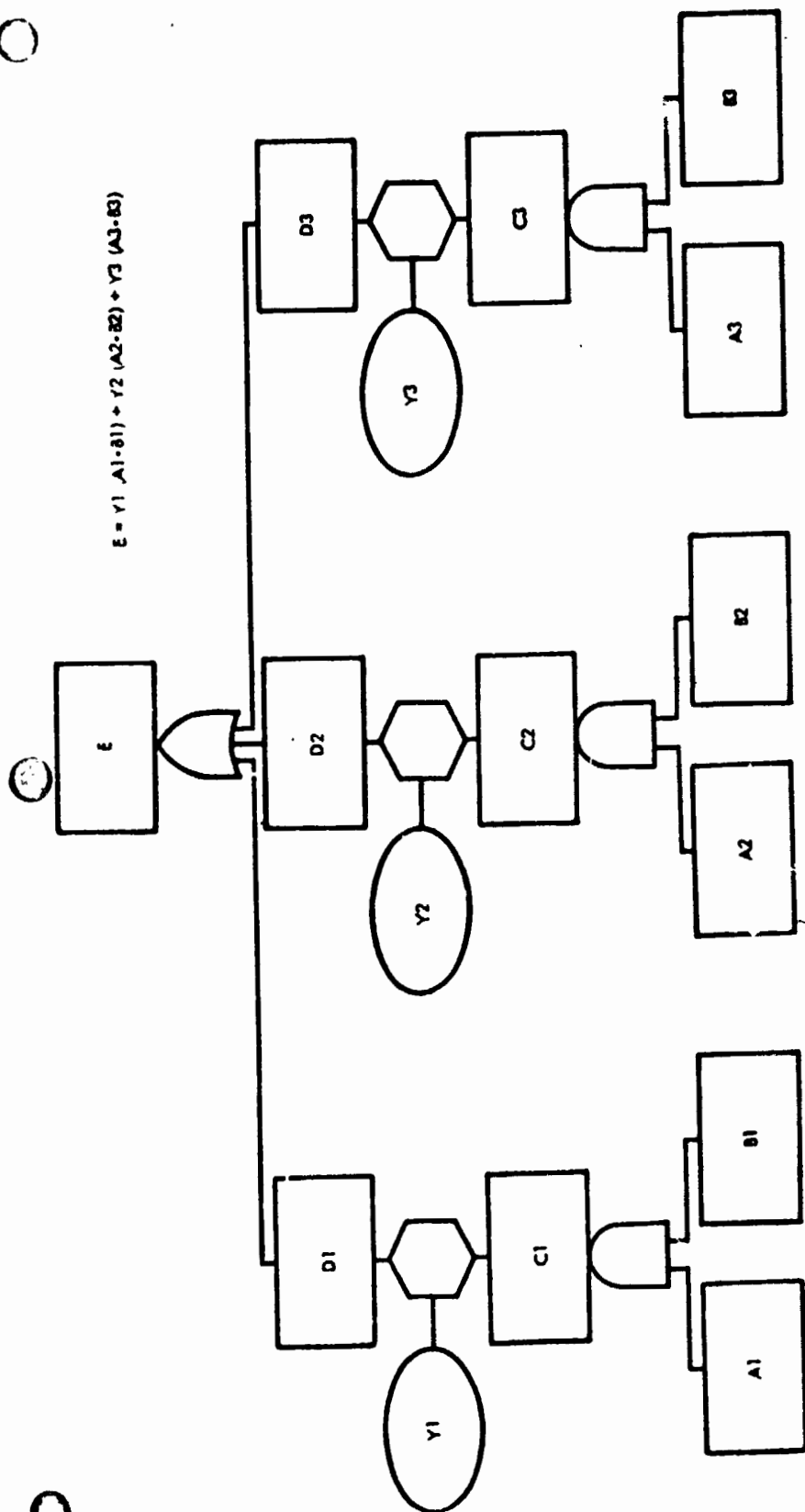
The probability numbers in the matrix should not be taken as the probability of two fault events being combined together. These numbers indicate the probability that two combined fault events will result in the undesired event after they have statistically been combined. Example 5 (Figure C7) shows the generalized case and the mathematical equations involved.

2.4.2.4 Conclusion

The preceding discussion provides evidence that the Matrix Gate and its associated matrix successfully represent a condition of similar or redundant fault event combinations in a simple and concise form while at the same time yielding all of the qualitative information involved.

USE FOR TYPEWRITTEN MATERIAL ONLY

Example 5



$$C1 = A1 \cdot B1$$

$$D1 = Y1(A1 \cdot B1)$$

	B1	B2	B3
A1	Y1	0	0
A2	0	Y2	0
A3	0	0	Y3

MATRIX

$$E = Y1(A1 \cdot B1) + Y2(A2 \cdot B2) + Y3(A3 \cdot B3) + \dots$$

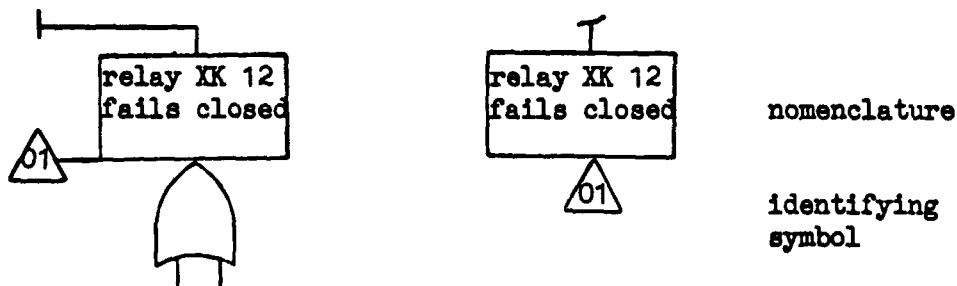
$$E = Y1(A1 \cdot B1) + Y2(A2 \cdot B2) + Y3(A3 \cdot B3)$$

Figure C7
Generalized Matrix Gate - Mathematical Equations

2.4.3

Transfer Symbols

The "transfer" symbol is used to allow continuity between two parts of a fault tree. A line drawn into the side of a triangle transfers everything below that triangle to another location, which is identified by a triangle with a line drawn from the apex and containing matching nomenclature and identifying symbol. The methodology is illustrated below:



Two types of transfer symbols exist. The "internal" (local) transfer symbol transfers portions of a fault tree only within a particular diagram. The idea behind this being that whenever the development of a certain portion of fault tree is identical in two or more places on the same diagram, it need only be developed in one place.

The "external" (global) transfer symbol transfers a portion of a fault tree to another, entirely separate, fault tree diagram. This happens when a development is identical for one event on two separate diagrams. Also, when a diagram is developed until there is no longer room for further expansion on the sheet (or it is desired to end at a particular place) an external transfer is used to continue development on another sheet. This is the method by which new fault tree developments (sub-diagrams) are started.

Figure C8 is an example of transfer symbol usage. It shows the correct use of both internal and external transfers.

USE FOR TYPEWRITTEN MATERIAL ONLY

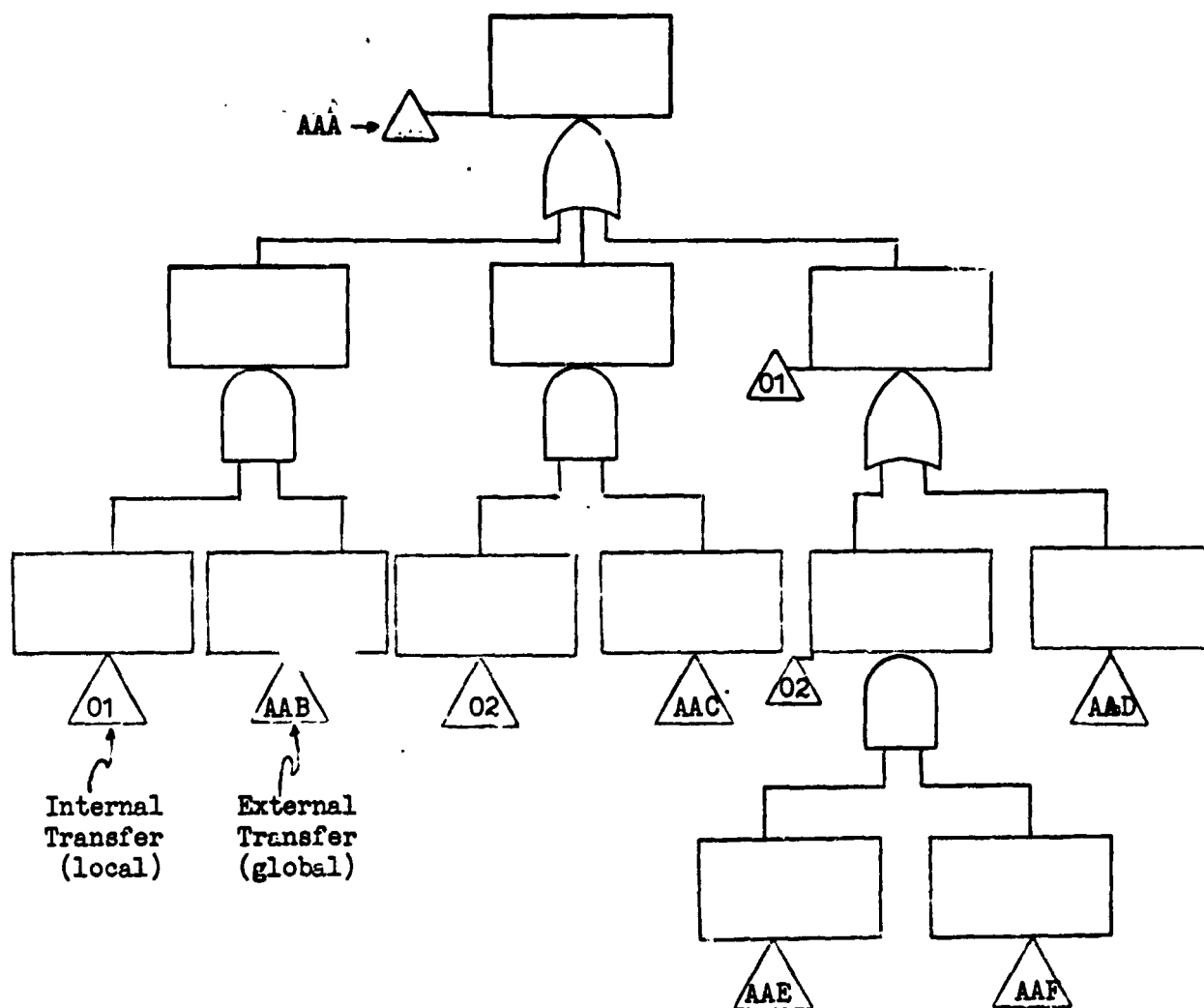
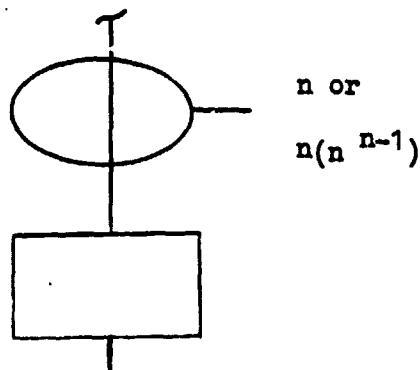


Figure C8
Transfer Symbol Usage

2.4.4 Output Encompassing Ellipse

An ellipse with a line extending out along the major axis is used when a component appears several times at the same place (e.g., a 10-stage counter where all 10 stages can be represented by illustrating one stage). Only one of the inputs is drawn to encompass the output. This indicates that the failure rate of that event is to be multiplied by the given factor (times 10 for the 10-stage counter) for an "OR" gate or raised to a given power and multiplies by the expression (n^{n-1}) for an "AND" gate. This symbol is illustrated below.

2.5 EVENT IDENTIFICATION

All events comprising a fault tree must be identified by a code. This is necessary for four reasons: 1) easy and precise referencing, 2) for purposes of machine drafting, 3) in order for a log of events to be maintained, and 4) for purposes of quantitative evaluation. The means by which events are identified is generally dependent upon the requirements and objectives of the particular analysis. A standardized procedure should be set up and adhered to for an entire analysis program.

The size and complexity of aerospace systems has demanded that a unique method of event identification be utilized. A method has been developed to satisfy the requirements and objectives of the Apollo system fault tree analysis, plus allowance for future expansion or quantitative evaluation.

All events are classified into one of two categories. These two categories are referred to as "global" events and "local" events. Global events are defined as events which are used on more than one fault tree diagram, and local events are defined as events which are unique to one fault tree diagram. The notation (or code) for events allows each event to be uniquely represented, at the same time differentiating between global and local events. The standardized notation is shown in Figure C9.

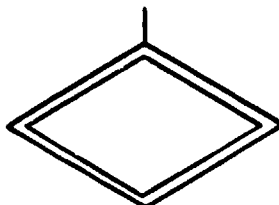
2.5

(Continued)

LOCAL EVENT

GLOBAL EVENT

V01
thru
V99



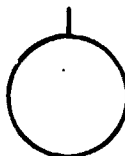
V100
thru
V999

W01
thru
W99



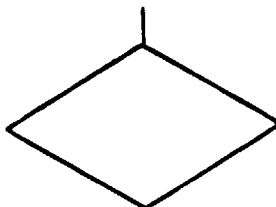
W100
thru
W999

X01
thru
X99



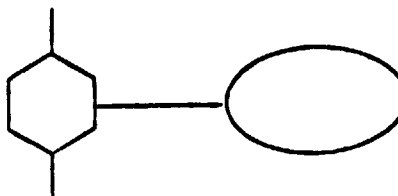
X100
thru
X999

Z01
thru
Z99



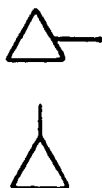
Z100
thru
Z999

Y01
thru
Y99



Y100
thru
Y999

01
thru
99



AAA
thru
ZZZ

USE FOR TYPEWRITTEN MATERIAL ONLY

Figure C9
Standardized Event Notation

2.5 (Continued)

From Figure C9, it can be readily discerned that the alpha character identifies the type of event. That is, "W" indicates a house, "X" indicates a circle, "Z" indicates a diamond, any "Y" indicates an oval. Local events are numbered from 01 through 99 for each and every diagram. For example, diamonds on the AAA diagram are randomly numbered as Z01, Z02, Z03, etc., and diamonds on the RAA diagram are also numbered as Z01, Z02, Z03, etc.. The only way to differentiate between local events is by indicating the fault tree diagram on which they are located. Global events are numbered from 100 through 999 and an index must be used to locate diagrams on which these events appear.

For the identification of global transfers (sub-diagrams) a three character alpha system is utilized. Using three alpha characters allows identifying nomenclature for a possibility of 17,576 diagrams. In conjunction with this method, a breakdown can be established which immediately identifies the source of each diagram. This breakdown consists of delegating the first letter, of all three letter combinations, to a particular MSF Center, contractor, or analyst.

As shown, local transfer symbols are numbered from 01 through 99 for each fault tree diagram. When referring to a particular local transfer, the diagram on which it appears must also be given.

2.6 BASIC DIAGRAM METHODOLOGY

The development of a fault tree diagram commences with the definition or identification of the top "undesired event" to be analyzed. The top undesired event can be an encompassing event, such as "mission loss", indicating a complete system analysis, it could be a limiting event, such as "crash due to engine failure", or it could be a specific event, such as "amplifier fails resulting in low output", indicating analysis beginning at a hardware level. Once definition of the undesired event has been accomplished, the system is analyzed using the following rules and definitions of fault tree diagramming to determine and model the inter-relationships and combinations of both normal and abnormal system functions which could cause the occurrence of the top undesired event.

The next step is to divide the system operating modes into phases. A phase is that increment of a system's life which can be analyzed independently, yet recognizing that there may be commonality of analysis between any of the phases. System phase breakdown should continue (corresponds to system engineering functional analysis) until the environment stays relatively constant through the phase element and system operational characteristics do not change the fault environment. The development of a fault tree proceeds through the identification and combination of the system events (normal and fault) until all fault events are definable in terms of basic identifiable hardware faults, to which failure rate data can be applied.

2.6

(Continued)

Figure C1C shows the general relationship of fault tree segments. Although shown as distinct elements, it should be noted that the segments will, to a certain extent, "mix" together throughout the fault tree structure.

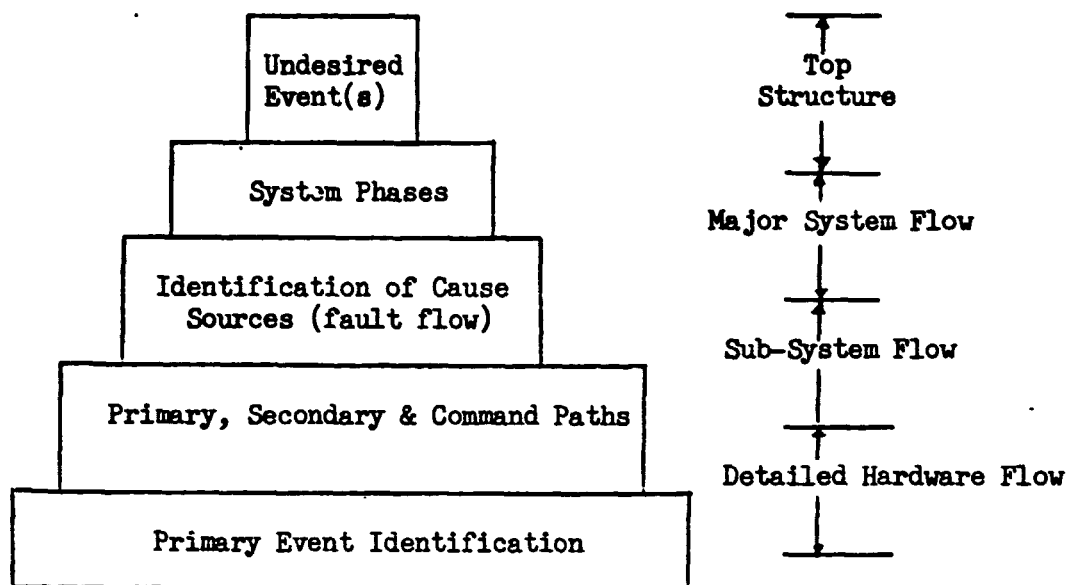


Figure C1C
Fault Tree

Developing the "fault flow," or cause and effect relationship of events through a system, requires deductive reasoning at each "gate event" or level of the fault tree. This deductive reasoning basically involves the answering of five questions: 1) necessity, 2) sufficiency, 3) primary, 4) secondary, and 5) command. These questions effectively develop the structure of the fault tree on a progressive, or level-by-level, basis.

To answer the questions "necessity" and "sufficiency" requires an evaluation of the system for normal and abnormal functional event relationships. This evaluation determines the system unique events, and logic gates combining them, to result in the undesired event. This is accomplished by looking at the undesired event and asking, "What is necessary and sufficient to cause this undesired event?" For example, an ordnance device will be activated when two events occur: 1) the ordnance device Safe and Arm mechanism closes, "AND" 2) energizing power is available on the ordnance device ignition line. These two events are all that is "necessary" and "sufficient" to cause activation of the ordnance device.

2.6

(Continued)

The questions "primary" and "secondary" are questions requiring an evaluation of the system to determine what primary and/or secondary fault events can occur to result in another fault event.

A concise definition of "primary" and "secondary" failures:

Primary Failure: Failure initiated by failures within, and of, the component under consideration, e.g., resulting from poor quality control during manufacture, etc., applied only to the component during Fault Tree Analysis when a generic failure rate is available.

Secondary Failure: Failure initiated by out of tolerance operational or environmental conditions, i.e., a component failure can be initiated by failure not originating within the component.

These questions also help to identify the specific failure modes of the fault event. For example, a primary failure mode of an ordnance device would be the mode of auto-ignition. A secondary failure mode would be that of ignition due to excessive external shock or heat.

The question "command" is really a guideline for development through the system. The question asks, "What upstream event will command the downstream event to occur?" The upstream event may be a primary and/or secondary event, or it may be an event commanded by an event further upstream.

A concise definition of "command" failure:

Command Failure:* The component was commanded/instructed to fail i.e., resulting from proper operation at the wrong time or place.

Essentially, the "command path" is a chain of events delineating the failure path of command events through a system. The command path ultimately results (at the finish of the analysis) as a primary and/or secondary fault event. Take for example, a set of relay contacts failing closed, as part of a system function. The contacts may fail closed as a primary failure, they may fail closed from a secondary cause such as foreign material bridging the contacts, or they may be commanded to close by a relay coil failure. If an upstream event causes the relay coil to be energized, the contacts are effectively "commanded" to close as a result of this upstream event.

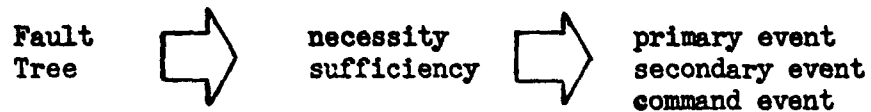
* Component may not always have command failure mode (e.g. a standard bolt) in which case this mode may be disregarded.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.6

(Continued)

The effective inter-relationship of the five necessary deductive questions is shown below:



As indicated, a fault tree is constructed of primary events, secondary events and command events through the medium of necessity and sufficiency.

In developing a fault tree certain thought processes take place in the mind of the analyst. The steps of development at each level of the fault tree delineating these thought processes are:

- 1) Define the undesired output event;
- 2) Determine what is "necessary and sufficient" to produce the undesired output;
- 3) List all primary events related to the undesired output;
- 4) List all secondary events related to the undesired output;
- 5) Define the undesired input event which could command the output event;
- 6) Repeat steps 1 - 5 for the new undesired event defined in step 5.

Figure C11 shows the relationship of the above steps to the structure of a fault tree. The inherent simplicity and logical process is readily apparent from this example.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.6

(Continued)

USE FOR TYPEWRITTEN MATERIAL ONLY

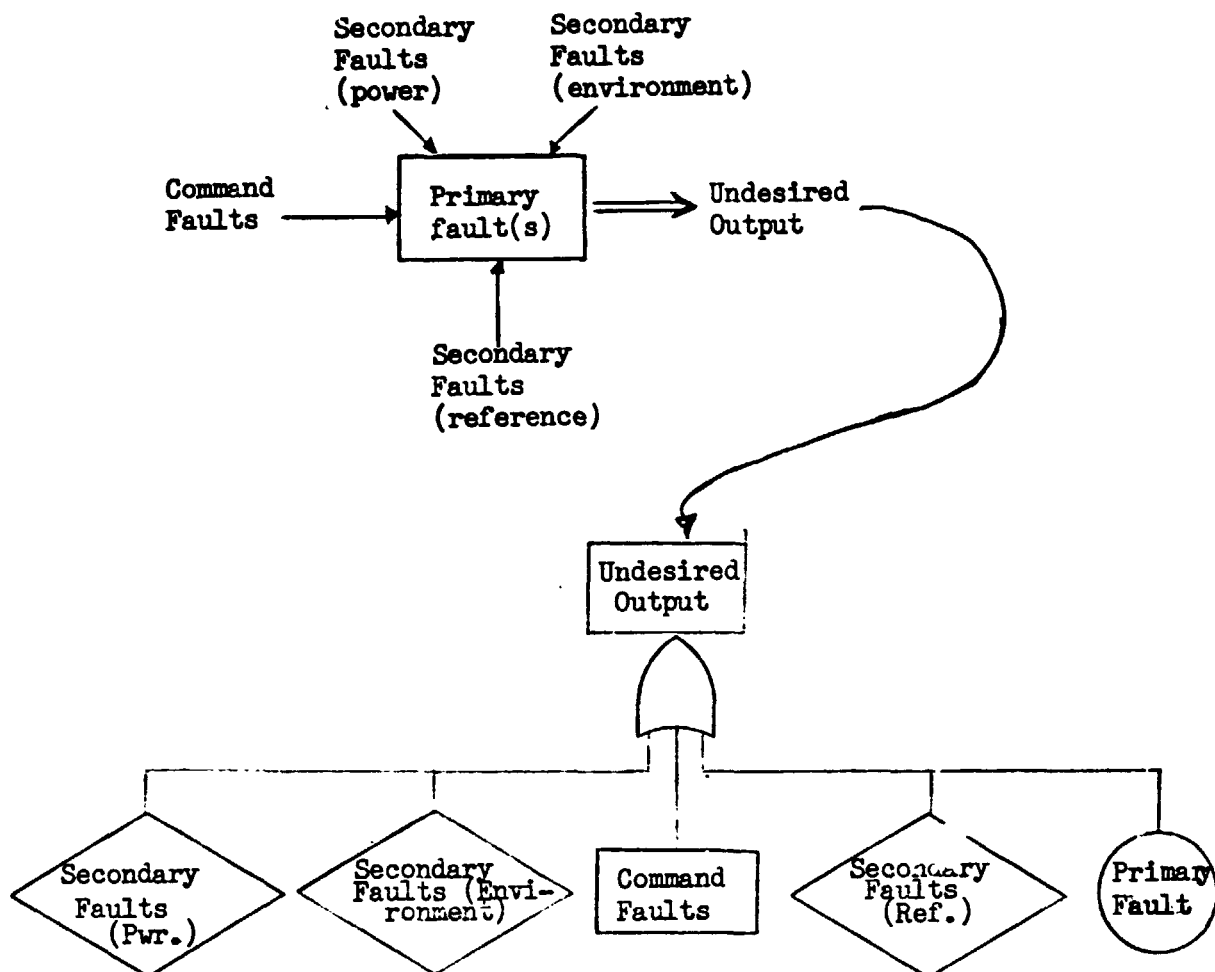


Figure C11
Fault Tree Relationships

2.6

(Continued)

Figure C12 shows a logic diagram structure which portrays the relationship of the command event to the primary and secondary events, and also how command events lead to a "command path." It must be remembered that the command path, as such, is only a guideline for analysis of event development through a system. Command events create an orderly and logical manner of analysis at each level of the fault tree. Once an analysis is completed, comparison between the fault tree and signal flow diagram will show that the fault tree "command path" of a branch will represent the steps of signal flow along a single thread.

USE FOR TYPEWRITTEN MATERIAL ONLY

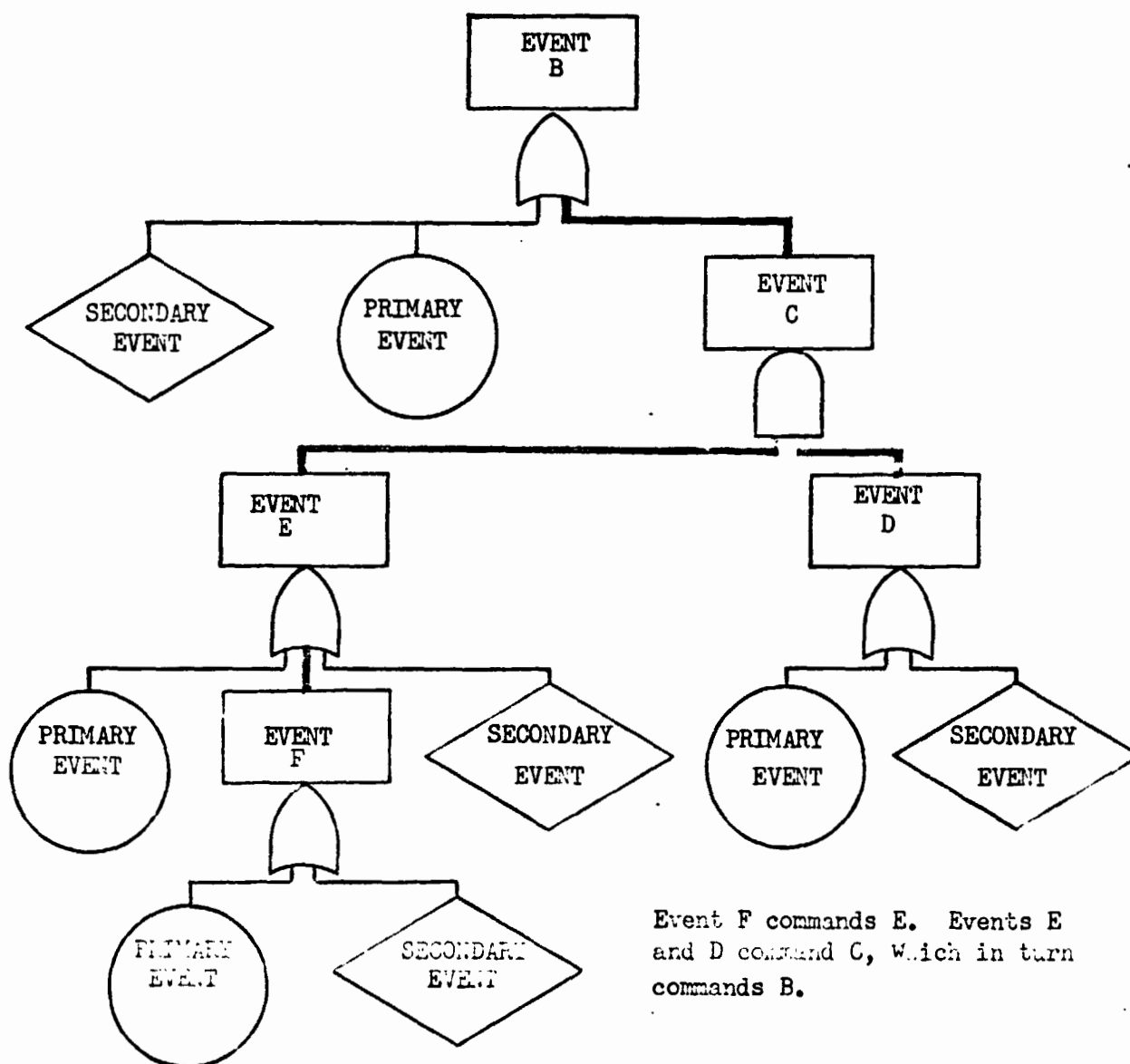


Figure C12
Example of Command Path

2.7

THE HUMAN ELEMENT

Any system which requires the human element in order to perform its intended function must have an analytical development that includes the human as part of the system. The human element is a complex subsystem, and human cause and effect relationships must be an integral part of the system's fault tree structure.

An example of how the human element can be portrayed in a fault tree is shown in Figure C13. The top event defines any arbitrary human operation and is used merely to illustrate the development below the event. The circle shown as "Crew Member Fails to Perform Function" (the identified critical function) represents the possibility of inadvertent error, usually highly improbable. The other two inputs to the top "OR" gate represent the "command" (no input information) development and the "secondary" cause development. Either of these two branches will most likely contain the dominant factors associated with failure of a crew member to perform a critical function. The events shown in this fault tree, Figure C13, are examples of the types of causes which could result in no action taken by a crew member. There are others which for simplicity are not shown in this illustration (indicated by dotted lines).

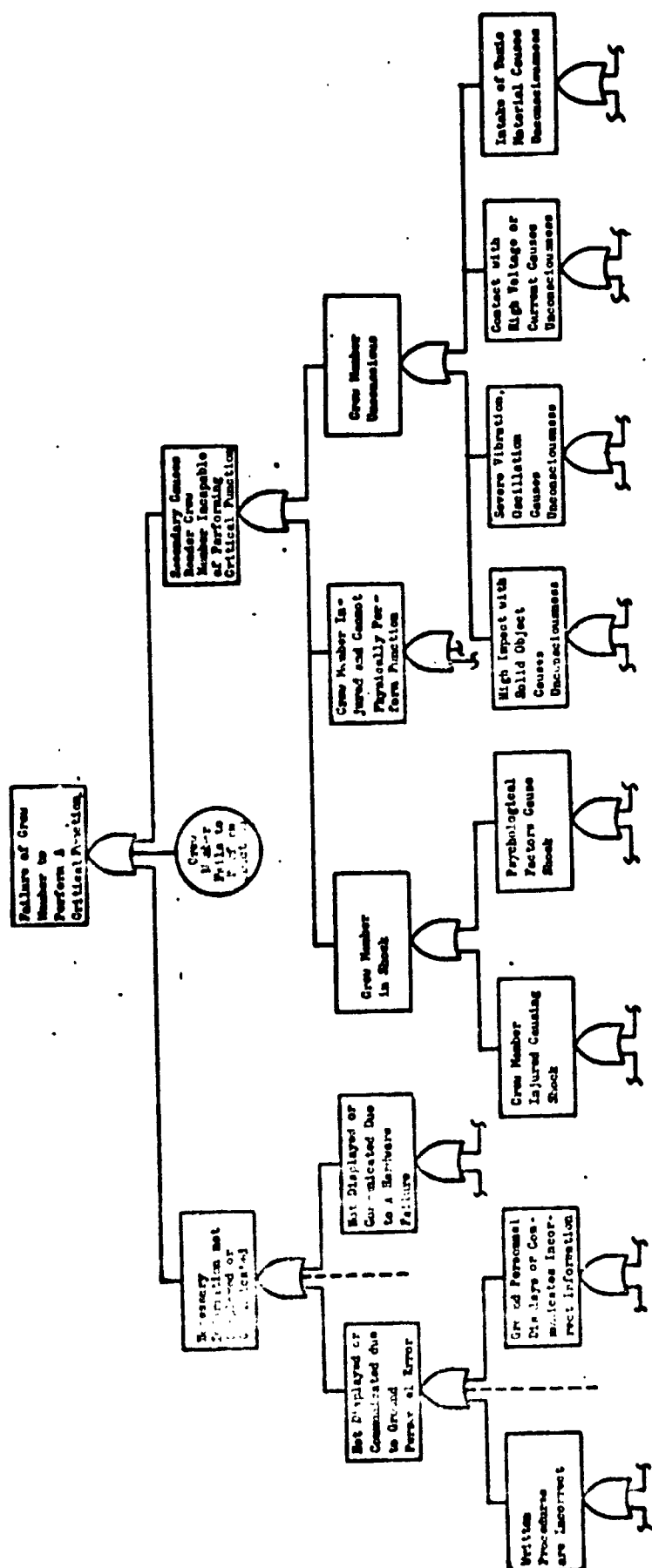
2.8

DOMINANT PATHS

A dominant path is the chain of events which is most "likely" to result in the undesired event (potential accident). In a typical case, there may be several paths of various degrees of dominance which can result in a given undesired event. These chains and their associated degrees of dominance are most clearly identified by the system safety model (fault tree or logic diagram). Dominant paths and their relative degrees of dominance are determined by event weighting (inspection) or rigorous mathematical solution of the model.

Since the dominant path is the most likely avenue along which the undesired event(s) can occur, the most cost effective approach is to concentrate the initial prevention effort in this area. It may be necessary to consider other paths within the model, in a descending order of dominance, in order to achieve an acceptable level of risk for the occurrence of a particular undesired event.

Preparing to locate dominant paths requires that the system safety model for a given undesired event (potential accident) has been developed to the extent necessary to identify dominant paths. As a minimum, the fault tree development, which is the model, must encompass all those safety features and devices which have been designed into the system. This assures that adequate consideration has been given to those areas of the system which are of the greatest "risk," since safety devices are normally placed where the greatest risk of an undesired event occurring exists.



HUMAN ELEMENT EXAMPLE

2.8 (Continued)

Logical inspection or mathematical processes determine the degree of dominance for those paths of the model which contribute the most to the likelihood of the undesired event. The term "logical inspection" is defined to mean the logical thought processes of a trained and experienced analyst being applied through examination of the model. These processes, associated with weighting factors he may consider, lead to the resulting statement by the analyst that "these events (identified) and path(s) appear to be the most probable."

The term "mathematical process" can be a solution of the model by any of several methods. Normally, a diagram with 250 events or less is solved by the Lambda-Tau (hand calculated) method, and a diagram with greater than 250 events on a digital computer using Monte Carlo simulation with importance sampling. An event in this case is defined to be any element of the diagram other than a logic gate. Since the purpose of the quantitative evaluation of a diagram is to identify dominant paths and their relative significance, the diagram is usually simplified by inspection to minimize the structure to be simulated. This inspection is the elimination of those events and branches which are obviously insignificant compared to others which are inputs to the same gate.

Control of dominant paths is accomplished by the following:

- 1) Establish a predetermined limit within which the initial path selection is bounded. This involves the identification of those paths which are computed to be above any established limit for the system.

If the paths are near or below the limit, then they are selected by picking those which are within an "order of magnitude" or so of the limit, or are of the same type.

- 2) The initial selection must be divided into groups for which a set of predetermined limits has been established for each grouping. The grouping of paths is accomplished by selecting those within an order of magnitude of each other or those which have an apparent commonality within the system.
- 3) Determine if a common point of departure exists among the paths of each group. This evaluation involves determining if there are common faults among the paths. Recommended changes to the system at these common points provides the most effective way to eliminate paths, or at least reduce them to an acceptable level.
- 4) Convert the fault tree dominant paths by grouping events at logical summary points. Conversion of the fault tree dominant paths involves making a listing of these events which, when "OR"-ed, result in an interim event. The method is to convert each path to a simplified alternating "AND," "OR," "AND," "OR," etc., relationship.

2.8

(Continued)

- 5) Simplify the fault tree of the dominant path by logically re-diagramming. Simplification involves re-diagramming the relationships summarized in step 4. This results in a simplified diagram of each path which can be readily correlated with a functional flow diagram of the system. The paths can now be verified as to accuracy and the actual fault points introduced into a functional flow diagram to show where and how the fault combinations affect system operation.
- 6) Determine those events for which a design change or the development of a procedure will best and most cost effectively reduce the probability of occurrence of an undesired event to an acceptable level of risk.
- 7) Insert alternative solutions as derived by steps 1 through 6 and repeat the process until an acceptable level of risk is obtained. This step involves working with designers and selecting several alternative system changes to reduce the probability of occurrence of each path. For each alternative to be evaluated, the fault tree is changed to reflect the change and the diagram is recomputed to determine the change impact. Care must be exercised to assure that other paths or branches of the tree which have the same event or fault sequence are also changed to reflect the change being evaluated.
- 8) Advise appropriate level of management of findings and recommendations.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9 FAULT TREE EVALUATION

2.9.1 Failure Data Development for Fault Tree Evaluation

Failure data is developed as a tool to define the effects of various component failure modes and classify these effects on system equipment or personnel. The format in Figure C14 is provided for assistance and guidance in developing system safety failure data. This format can be changed according to various requirements and should be considered as an example only.

The various columns are explained as follows:

COLUMN I - COMPONENT

Components are defined, at the discretion of the analyst, by their physical or functional significance. The following guide will facilitate understanding of the types of natural separations to consider. It is not intended to be exhaustive.

1) Electronic Logic Circuits

Many systems or subsystems are made up of a number of basic circuit designs which perform an identifiable purpose. These are used as building blocks for larger circuits designed to perform the required logic functions of the system or subsystem. To minimize the analysis required, the basic circuits can be defined as major components, and an analysis made of each logic function.

2) Mechanical Devices

Mechanical devices can be either a single part or an assembly of parts which perform one function. The use in the system will dictate to what level of detail mechanical parts should be considered. Single parts which can be considered major components are: solid driveshafts, engine blocks, primary structure, etc.. The majority of mechanical devices will be assemblies of many parts and it is more reasonable to treat the assemblies as major components, for example: relays, pumps, motors, mechanical safety devices, etc.. This permits the majority of vendor-supplied mechanical devices to be analyzed as major components.

3) Electrical Systems

Major components can be basic components of a circuit or combinations of components used to perform one single function such as amplifiers, rectifiers, or regulators. The level of data development should be based on the importance of the part as a functional element in the design.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

I COMPONENT	II COMPONENT FAILURE MODE	III FAILURE RATE	IV SOURCE OF DATA	V COMPONENT FAILURE STATE	VI EFFECT OF COMPONENT FAILURE	VII REMARKS
<div>FIGURE - C14</div> <div>Fault Tree Failure Data Format</div>						

2.9.1 (Continued)

4) Chemical Systems

In systems containing chemical compounds, the chemicals should be considered as major components if these compounds can cause failures of other components through chemical reaction or release of chemical energy. Examples of chemical components are: fuels, pressurants, coolants, and preservatives.

5) Safety Devices

Safety devices will normally be considered major components since they are used primarily to protect against undesired events.

6) Wiring

Interconnecting wiring of major components will be considered a major component. Internal wiring will be considered as a part of a major component. Physical characteristics of cables which circumvent failures between wires should be stated in the cable analysis.

COLUMN II - COMPONENT FAILURE MODE

Failures of major components consisting of one part require a listing of the modes in which that part may fail. Failures of major components consisting of more than one part will require a failure mode and effects analysis to determine how the failure modes of each part affect the components' output. These part failure effects will be the failure modes of the major component listed in the system safety failure data. All failure modes of the component should be listed.

COLUMN III - COMPONENT FAILURE RATE

The predicted reliability of the failure rate computed from actual field data of primary failures should be tabulated in this column for each major component in each of its modes of failure. This data can be used in evaluating the probability of the fault event or in selecting which critical or catastrophic events should be analyzed if the decision is made not to analyze an event so classified. It also serves as a data bank for future reference when the need arises to analyze other undesired events as a result of system changes.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.1 (Continued)

COLUMN IV - SOURCE OF DATA

This column states the source of the failure rate data. It shows the differentiation between field data, test data, calculated data, etc..

COLUMN V - FAILURE STATE

Many major components are recurrently activated during the system's operational life. The level of stress on these components will change from one system mode to another. The effect of a failure in each mode can be different; for example, components supplied with power only during a test can create a fault hazard only while a test is performed. Failures existing in one mode of system operations can also adversely affect the system when the mode is changed. This column therefore should reflect the environmental state of the component when it failed.

COLUMN VI - EFFECT OF COMPONENT FAILURE

This column states the effect on related system equipment and/or personnel due to the component failure.

COLUMN VII - REMARKS

This column may be used to include additional information needed to clarify or verify information in other columns as well as other information currently pertinent to system safety efforts.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.2

Fault Tree Quantitative Evaluation

After the fault tree has been constructed and input data acquired, the tree can be evaluated. The object is to establish the likelihood of occurrence of the "undesired event" and to evaluate the relative contribution of each indicated failure mode. With this information the safety analyst can identify the dominant system failure modes (dominant paths) and management can make the decision as to whether or not corrective action is warranted.

Two basic approaches used to quantify fault trees are 1) calculation, and 2) simulation. The calculation or deterministic approach will be considered first. For fault trees where every basic input is non-repairable, classical probability can be used. In this case, each gate merely represents the operation to be performed (i.e., union for "OR" gates and intersection for "AND" gates). The classical probability approach, while simple and efficient, is not adequate for fault trees where the effects of a basic failure can be eliminated before causing the undesired event. A basic failure whose effect can be removed is called repairable; however, the usage of the word "repairable" is irregular because the effect may be terminated without actually repairing or replacing the failed item. A more definitive time is "fault duration time." The analysis of repairable systems requires special statistical techniques.

2.9.2.1

Computation

One technique in the calculation or deterministic approach is the "Lambda-Tau" method to evaluate fault trees. In this method, failure rates must be small, fault duration times must be small with regard to mission length, and redundant inputs must be removed. Redundancies that are not removed may lead to serious unbounded errors in the answer. The fault tree diagrams are usually expressed algebraically and operated on by theorems of Boolean algebra to remove redundancies. The "Lambda-Tau" method can be applied by hand or by digital computer. However, as the fault trees get larger in size, the task of hand calculation becomes time consuming, laborious and error prone. A computer program can write the algebraic expression and can use Boolean algebra to remove the redundancies. However, computer core storage on most computers limits the size of the tree solvable by this method. Nevertheless, smaller fault trees can be calculated accurately by hand or computer using "Lambda-Tau" methods. (See Section 2.9.3 for further details.)

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.2.2 Simulation

In the simulation approach, a fault tree is represented on a computer and failures are simulated over a given mission length. The computer prints out the failure which leads to the undesired event, and the probability is calculated. The simulation approach has all the advantages of the calculation approach except for the greater amount of computer time needed to simulate fault trees with small probabilities. Simulation offers several advantages: namely, the dominant paths are listed and the computer can solve larger diagrams (10 times larger than "Lambda-Tau"). Simulation has gone through many stages of development. In its early stages, the amount of computer time required became prohibitive; however, special Monte Carlo variance reducing techniques (importance sampling) have reduced greatly the computer time required. The importance sampling technique distorts the true failure distribution to make events occur more rapidly. Thus, the number of trials (a trial represents the predefined mission length of the system) required for an acceptable statistical confidence is reduced. With fewer trials required, computer time is reduced. The distortion of the distribution, when using importance sampling, is compensated for by calculation weight factors. See Nagel, P.M., and Schroder, R.J., "The Efficient Simulation of Rare Events in Complex Systems", D2-114072-1, The Boeing Company. Overall, simulation offers more potential and has proven to be more effective in calculating accurate answers than the "Lambda-Tau" calculation method.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3 Constant Repair or "Lambda Tau" Method of Fault Tree Evaluation

2.9.3.1 Coexistence of Independent Failures

Suppose there is given a group of n repairable items, and these items may or may not fail in a given time period, T . Let event A_1 represent the failure of item 1, event A_2 the failure of item 2, and in general event A_i the failure of item i , $i = 1, 2, \dots, n$. These failures are chance failures, occurring at random and independent of each other. It is these chance failures which have an exponential distribution of their time to failure. Hence the probability that an item in that group will not fail may be expressed as the reliability,

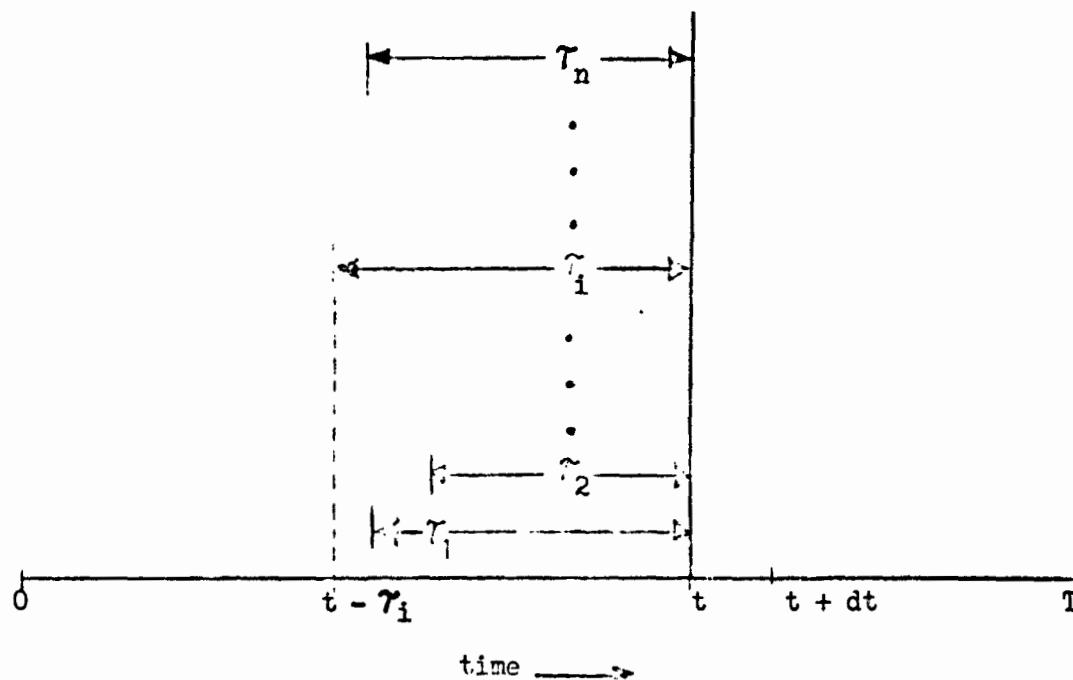
$$R_i(t) = e^{-\lambda_i t_i} \quad (1)$$

where t_i is the given time period, and λ_i is the number of failures per unit time. The unreliability or chance of failure is

$$Q_i(t) = 1 - R_i(t) = 1 - e^{-\lambda_i t_i} \quad (2)$$

This unreliability may also be called the probability that item i will fail during time t_i , and is the probability that event A_i will happen. For each item i assume that the failure rate λ_i and repair time τ_i are constant. Further assume that τ_i/T , λ_i , and $\lambda_i \tau_i$ are small.

Consider an interval of time from 0 to T as shown in the figure below.



2.9.3.1 (Continued)

In order for a failure to exist in the small time interval dt , the failure must occur either in the small interval dt , or in some time interval from $t - \tau_1$ to t . If the failure occurs before $t - \tau_1$, it will be repaired before it can exist in the dt interval; and if it occurs after $t + dt$, it cannot possibly exist in the dt interval. The probability of event A_1 happening in the τ_1 period is $(1 - e^{-\lambda_1 \tau_1})$. The probability of event A_1 happening in the dt time interval is $\lambda_1 dt$. These are the only two ways in which the event A_1 can happen. The probability for all events, A_1, A_2, \dots, A_n to coexist in the dt interval is given by

$$\begin{aligned} Hdt = & \lambda_1 dt (1 - e^{-\lambda_2 \tau_2}) (1 - e^{-\lambda_3 \tau_3}) \dots (1 - e^{-\lambda_n \tau_n}) \\ & + \lambda_2 dt (1 - e^{-\lambda_1 \tau_1}) (1 - e^{-\lambda_3 \tau_3}) \dots (1 - e^{-\lambda_n \tau_n}) \\ & \cdot \\ & \cdot \\ & + \lambda_n dt (1 - e^{-\lambda_1 \tau_1}) (1 - e^{-\lambda_2 \tau_2}) \dots (1 - e^{-\lambda_{n-1} \tau_{n-1}}) \end{aligned} \quad (3)$$

Consider the first term in this formula, which is the probability that event A_1 occurs during dt and coexists with the other failures having occurred previous to t . The probability of event A_1 occurring in dt is $\lambda_1 dt$, and the probability of occurrence A_2 during period τ_2 previous to t is $(1 - e^{-\lambda_2 \tau_2})$. The product of these probabilities for events A_1 through A_n gives the probability of the coexistence of all events, where only A_1 occurs during dt . The second term gives the probability of the coexistence of A_1, A_2, \dots, A_n where only A_2 occurs during the interval dt . The sum of these n terms equals the probability of n events coexisting during dt interval.

Let $f(t)$ be the probability that A_1, A_2, \dots, A_n have not coexisted up to time t . Then $f(t + dt)$ expresses the probability that A_1, A_2, \dots, A_n have not coexisted from time 0 to $t + dt$. This can be expressed as

$$f(t + dt) = f(t) (1 - Hdt) \quad (4)$$

Where $f(t + dt)$ equals the product of the probability of no coexistence of the items A_1 through A_n from 0 to t , $f(t)$, and the probability of no coexistence of the items A_1 through A_n from time t to $t + dt$, $(1 - Hdt)$.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3.1 (Continued)

By definition, the differential of $f(t)$ is $f(t+dt)-f(t)$; therefore:

$$df(t) = f(t) (1 - Hdt) - f(t)$$

$$df(t) = -f(t) Hdt$$

$$\text{and } \frac{df(t)}{f(t)} = -Hdt$$

Solving this differential equation by integration,

$$\ln f(t) = -Ht + C \quad (5)$$

At time zero, the probability that A_1, A_2, \dots, A_n have not coexisted is equal to 1. Then $f(t) = 1$ when $t=0$, and $\ln(1)=C$. Since $\ln(1) = 0$, then, from (5)

$$\begin{aligned} \ln f(t) &= -HT \\ f(t) &= e^{-HT} \end{aligned} \quad (6)$$

The probability that events A_1 through A_n have coexisted at some time t is

$$P(A) = 1 - f(t) = 1 - e^{-HT}$$

For sufficiently small HT ,

$$P(A) \sim HT. \quad (7)$$

Hence $P(A) \sim HT = (\lambda_1 \lambda_2 \tau_2 \lambda_3 \tau_3 \dots \lambda_n \tau_n$

$$+ \lambda_2 \lambda_1 \tau_1 \lambda_3 \tau_3 \dots \lambda_n \tau_n$$

.

.

.

$$+ \lambda_n \lambda_1 \tau_1 \lambda_2 \tau_2 \dots \lambda_{n-1} \tau_{n-1}) T \quad (8)$$

$$= \lambda_1 \lambda_2 \dots \lambda_n (\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots$$

$$\tau_n + \dots + \tau_1 \tau_2 \dots \tau_{n-1}) T$$

2.9.3.2 "AND" GATE λ

The form of the probability figure for the coexistence of failures A_1, A_2, \dots, A_n , suggests that the failure rate for all these events is

$$\lambda_n = \lambda_1 \lambda_2 \dots \lambda_n (\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots \tau_n + \dots \tau_1 \tau_2 \dots \tau_{n-1})$$

2.9.3.3 "AND" GATE γ

Consider a situation in which events A_1, A_2, \dots, A_{n+1} must coexist to produce an undesired event. No output will occur for the duration of the time τ_n when only events A_1, A_2, \dots, A_n coexist. Let λ_n be the failure rate and τ_n the effective period of coexistence of failures A_1 through A_n . An expression for the period τ_n is derived as follows:

$$\lambda_n \lambda_{n+1} (\tau_n + \tau_{n+1}) = \lambda_1 \lambda_2 \dots \lambda_{n+1} (\tau_2 \tau_3 \dots \tau_{n+1} + \dots \tau_1 \tau_2 \dots \tau_n) \dots$$

$$\text{Since } \lambda_n = \lambda_1 \lambda_2 \dots \lambda_n (\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots \tau_n + \dots \tau_1 \tau_2 \dots \tau_{n-1})$$

$$\text{Then } \lambda_1 \lambda_2 \dots \lambda_n (\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots \tau_n + \dots \tau_1 \tau_2 \dots \tau_{n-1})$$

$$\lambda_{n+1} (\tau_n + \tau_{n+1}) =$$

$$\lambda_1 \lambda_2 \dots \lambda_{n+1} (\tau_2 \tau_3 \dots \tau_{n+1} + \tau_1 \tau_3 \dots \tau_{n+1} + \dots + \tau_1 \tau_2 \dots \tau_n)$$

Therefore:

$$\tau_n = \frac{\tau_1 \tau_2 \dots \tau_n}{\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots \tau_n + \tau_{n+1} \tau_1 \tau_2 \dots \tau_{n-1}} = \frac{1}{\frac{1}{\tau_1} + \frac{1}{\tau_2} + \dots + \frac{1}{\tau_n}}$$

by mathematical induction.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3.4 "OR" GATE λ

Considering the same group of n items, $i = 1, 2, \dots, n$, the probability that none of the events occurs during time period T is given by

$$R_i(t) = e^{-\lambda_1 T} e^{-\lambda_2 T} e^{-\lambda_3 T} \dots e^{-\lambda_n T}$$

$$R_i(t) = e^{-(\lambda_1 + \lambda_2 + \dots + \lambda_n) T}$$

Hence the probability that any one of the events occurs is

$$Q_i(t) = 1 - R_i(t) = 1 - e^{-(\lambda_1 + \lambda_2 + \dots + \lambda_n) T}$$

Therefore the failure rate for the occurrence of any event in the time interval is $\lambda_u = \lambda_1 + \lambda_2 + \dots + \lambda_n$ from the general form of the reliability equation.

2.9.3.5 "OR" GATE τ

To find the effective duration for the condition that any one of the group of items may fail in the time period, consider the following example. Let any one of the events A_1, A_2, \dots, A_n coexist with an event A_{n+1} . Let λ_u and τ_u represent respectively the failure rate and effectivity time obtained from the union of events A_1 to A_n , when event A_1 or A_2 or A_3, \dots, A_n occur in the given time interval. If these events A_1, A_2, \dots, A_n occur with event A_{n+1} , the result is $\lambda_u \lambda_{n+1} (\tau_u + \tau_{n+1})$ from the coexistence of failures discussion, and

$$\begin{aligned} \lambda_u \lambda_{n+1} (\tau_u + \tau_{n+1}) &= \lambda_1 \lambda_{n+1} (\tau_1 + \tau_{n+1}) + \lambda_2 \lambda_{n+1} (\tau_2 + \tau_{n+1}) + \dots \\ &\quad + \lambda_n \lambda_{n+1} (\tau_n + \tau_{n+1}) \end{aligned}$$

$$\text{Since } \lambda_u = \lambda_1 + \lambda_2 + \dots + \lambda_n$$

Then

$$(\lambda_1 + \lambda_2 + \dots + \lambda_n) \lambda_{n+1} (\tau_u + \tau_{n+1}) = \lambda_1 \lambda_{n+1} (\tau_1 + \tau_{n+1}) + \lambda_2 \lambda_{n+1} (\tau_2 + \tau_{n+1}) +$$

$$\text{Therefore } \dots + \lambda_n \lambda_{n+1} (\tau_n + \tau_{n+1})$$

$$\tau_u = \frac{\lambda_1 \tau_1 + \lambda_2 \tau_2 + \dots + \lambda_n \tau_n}{\lambda_1 + \lambda_2 + \dots + \lambda_n}$$

The outputs of the AND and OR gates are given in tabular form at the end of this paper.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3.6 Failures Occuring in a Given Order

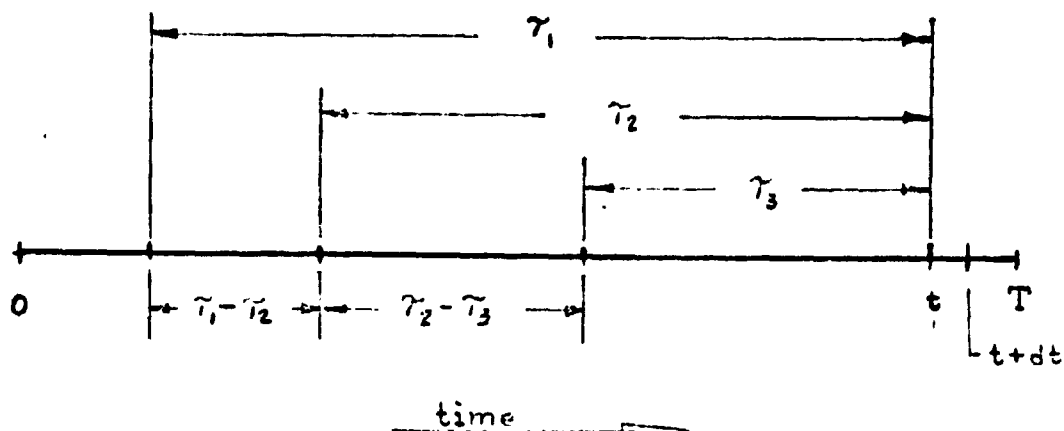
The probability expression for n items failing in an interval of time in a given order will be derived in the following discussion, and an approximation for small $\lambda\tau$ will be shown.

Consider a group of n items, A_1, A_2, \dots, A_n , each working at the beginning of an arbitrary interval of time, τ . Let $\lambda_1, \lambda_2, \dots, \lambda_n$ be the respective failure rates of the n items, and suppose that $\lambda_1\tau, \dots, \lambda_n\tau$ are very small. Let E be the event which occurs when A_1, A_2, \dots, A_n all fail in some specified order, e.g., A_1 occurs, then A_2 , then A_3 , etc., then

$$P(E) \sim \frac{\lambda_1 \lambda_2 \dots \lambda_n \tau^n}{n!}$$

In previous discussion, the expression $\frac{\lambda_1 \lambda_2 \lambda_3 \dots \lambda_n \tau^n}{n!}$ was obtained for the probability of occurrence of n events A_1, A_2, \dots, A_n in a particular order over a time period τ . Using these results, the probability will now be obtained for the occurrence of four events in order over a time period T when repair times are unequal

Let four events A_1, A_2, A_3, A_4 have respective repair times $\tau_1, \tau_2, \tau_3, \tau_4$ and failure rates $\lambda_1, \lambda_2, \lambda_3, \lambda_4$. Let the magnitudes of the repair times have the relationship, $\tau_1 > \tau_2 > \tau_3 > \tau_4$, as shown below



2.9.3.6 (Continued)

For this particular example event A_1 shall occur first, then A_2 , then A_3 , then A_4 . Events A_1 , A_2 , and A_3 shall occur prior to t and event A_4 shall occur in the dt interval. The probability of A_4 occurring in the dt interval is $\lambda_4 dt$. To coexist with A_4 in the dt interval, A_1 , A_2 , and A_3 can occur in the five following ways:

- a. A_1 occurs in interval $\tau_1 - \tau_2$, A_2 occurs in interval $\tau_2 - \tau_3$, and A_3 occurs in interval τ_3

$$P(a) = \lambda_1(\tau_1 - \tau_2) \lambda_2(\tau_2 - \tau_3) \lambda_3 \tau_3$$

- b. A_1 occurs in interval $\tau_1 - \tau_2$ and A_2 and A_3 both occur in order in interval τ_3

$$P(b) = \lambda_1(\tau_1 - \tau_2) \frac{\lambda_2 \lambda_3 \tau_3^2}{2}$$

- c. A_1 and A_2 both occur in order in the interval $\tau_2 - \tau_3$ and A_3 occurs in the interval τ_3

$$P(c) = \frac{\lambda_1 \lambda_2 (\tau_2 - \tau_3)^2}{2} \lambda_3 \tau_3$$

- d. A_1 occurs in interval $(\tau_2 - \tau_3)$ and A_2 and A_3 occur in order in the interval τ_3

$$P(d) = \lambda_1(\tau_2 - \tau_3) \frac{\lambda_2 \lambda_3 \tau_3^2}{2}$$

- e. A_1 , and A_2 and A_3 all occur in order in the interval τ_3

$$P(e) = \frac{\lambda_1 \lambda_2 \lambda_3 \tau_3^3}{6}$$

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3.6 (Continued)

The total probability, $P(t)$, for the occurrence of A_1, A_2, A_3 in order is the sum of these probabilities

$$P(t) = P(a) + P(b) + P(c) + P(d) \\ = \lambda_1 \lambda_2 \lambda_3 (\tau_1 \tau_2 \tau_3 - \frac{\tau_1 \tau_3^2}{2} - \frac{\tau_2^2 \tau_3}{2} + \frac{\tau_3^3}{6}) .$$

The product of $P(t)$ and $\lambda_4 dt$ therefore, gives the probability that A_1, A_2, A_3, A_4 occur in the given order and coexist for the first time in the dt interval. If $f(t)$ is defined as the probability that A_1, A_2, A_3, A_4 have not occurred up to time t in a given order, and $f(t+dt)$ is the probability of A_1, A_2, A_3 , and A_4 have not occurred up to time $t+dt$ in a given order, then

$$f(t+dt) = f(t) (1 - P(t) \lambda_4 dt)$$

Since $P(t) \lambda_4 dt$ gives the probability that A_1, A_2, A_3, A_4 occur in the given order, $1 - P(t) \lambda_4 dt$ gives the probability that they do not occur as specified.

$$f(t+dt) - ft = - f(t) P(t) \lambda_4 dt$$

$$df(t) = - f(t) P(t) \lambda_4 dt$$

$$\frac{df(t)}{f(t)} = - P(t) \lambda_4 dt$$

$$\ln f(t) = - P(t) \lambda_4 \int_0^t dt = - P(t) \lambda_4 T$$

$$f(t0) = e$$

$$1-f(t) = 1 - e^{-P(t) \lambda_4 T}$$

If $P(T) \lambda_4 T$ is small, then the probability of the occurrence of this chain of events over time T , $P(1234)$ is

$$P(1234) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\tau_1 \tau_2 \tau_3 - \frac{\tau_1 \tau_3^2}{2} - \frac{\tau_2^2 \tau_3}{2} + \frac{\tau_3^3}{6}) T$$

2.9.3.6 (Continued)

By similar manipulations, the probability for the occurrence of A_1, A_2, A_3, A_4 in that order is

$$P(2134) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 \left[\frac{\tau_2 \tau_3^2}{2} - \frac{\tau_2 \tau_3^2}{2} + \frac{\tau_3^3}{6} \right] T$$

Similarly

$$P(2314) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 \left[\frac{\tau_2 \tau_3^2}{2} - \frac{\tau_3^3}{2} + \frac{\tau_3^3}{6} \right] T$$

$$P(3214) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 \frac{\tau_3^3}{6} T$$

$$P(3124) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 \frac{\tau_3^3}{6} T$$

$$P(1324) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 \left[\frac{\tau_1 \tau_3^2}{2} - \frac{\tau_3^3}{2} + \frac{\tau_3^3}{6} \right] T$$

The sum of these probabilities is

$$P(4) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\tau_1 \tau_2 \tau_3) T$$

If A_3 is the last event, τ_4 takes the place of τ_3 on the figure and the resulting probability is

$$P(3) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\tau_1 \tau_2 \tau_4) T$$

Similarly if A_2 and A_1 are respectively the last events, the associated probabilities are

$$P(2) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\tau_1 \tau_3 \tau_4) T$$

$$P(1) = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\tau_2 \tau_3 \tau_4) T$$

USE FOR TYPEWRITTEN MATERIAL ONLY

2.9.3.6 (Continued)

These probabilities may be added $P(1)$, $P(2)$, $P(3)$, and $P(4)$ mutually exclusive) giving the total probability of the coexistence of A_1 , A_2 , A_3 , and A_4 .

$$P = \lambda_1 \lambda_2 \lambda_3 \lambda_4 (\bar{\tau}_1 \bar{\tau}_2 \bar{\tau}_3 + \bar{\tau}_1 \bar{\tau}_2 \bar{\tau}_4 + \bar{\tau}_1 \bar{\tau}_3 \bar{\tau}_4 + \bar{\tau}_2 \bar{\tau}_3 \bar{\tau}_4) T$$

It is to be noted that this is equivalent to the coexistence formula. Thus, the probability for the coexistence of events can be obtained as the sum of the probabilities of each ordered chain of events.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

		2 INPUTS	3 INPUTS	INPUTS
A N D	γ^s UNEQUAL	λ_n	$\lambda_1 \lambda_2 (\gamma_1 + \gamma_2)$	$\lambda_1 \lambda_2 \dots \lambda_n (\gamma_1 \gamma_2 \dots \gamma_n + \gamma_1 \gamma_2 \dots \gamma_{n-1})$
		τ_n	$\frac{\tau_1 \tau_2}{\tau_1 + \tau_2}$	$\frac{1}{\frac{1}{\tau_1} + \frac{1}{\tau_2} + \dots + \frac{1}{\tau_n}}$
	γ^s EQUAL	λ_n	$2\lambda_1 \lambda_2$	$n\lambda_1 \lambda_2 \dots \lambda_n \gamma^{n-1}$
		τ_n	$\frac{\tau}{2}$	$\frac{\tau}{n}$
O R	γ^s UNEQUAL	λ_u	$\lambda_1 + \lambda_2$	$\lambda_1 + \lambda_2 + \dots + \lambda_n$
		τ_u	$\frac{\lambda_1 \tau_1 + \lambda_2 \tau_2}{\lambda_1 + \lambda_2}$	$\frac{\lambda_1 \tau_1 + \lambda_2 \tau_2 + \dots + \lambda_n \tau_n}{\lambda_1 + \lambda_2 + \dots + \lambda_n}$
	γ^s EQUAL	λ_u	$\lambda_1 + \lambda_2$	$\lambda_1 + \lambda_2 + \dots + \lambda_n$
		τ_u	τ	τ

Figure C1 5

2.10

REFERENCES

Document D2-117018-1
The Boeing Company
June 1968

Apollo Logic Diagram
Analysis Guideline

A. B. Mearns
Bell Telephone Laboratories, Inc.
June 1965

Fault Tree Analysis:
The Study of Unlikely
Events in Complex
Systems

Document D6-53604
The Boeing Company
November 1968

Fault Tree For Safety

Sales Literature by
California Computer Products, Inc.

Digital Plotting -
Computerized Machine
Drafting

Report No. ASR-69-1
The Boeing Company
June 1969

Fault Tree Analysis -
Methodology and Application

Space and Missile Safety
Organizations
U.S. Air Force
November 1968

SAMSO Exhibit 68-8

Document D2-84303-1
The Boeing Company
February 1967

System Safety Engineering
Analysis Techniques

Document D6A10784-3
The Boeing Company

Supersonic Transport
Fault Tree Procedures
Manual

USE FOR TYPEWRITTEN MATERIAL ONLY

APPENDIX D

FRACTURE MECHANICS ASSESSMENT

<u>Paragraph</u>	<u>CONTENTS</u>	<u>Page</u>
	List of Figures	D-002
1.0	Introduction	D-101
1.1	Application to Safety Analysis	D-101
1.2	Discussion of Analysis Method	D-101
1.2.1	Symbols	D-101
1.2.2	General	D-102
2.0	Prediction of Cyclic Life for a Thick-Walled Vessel	D-201
3.0	Prediction of Cyclic Life for a Thin-Walled Vessel	D-301
3.1	Background	D-301
3.2	Approach	D-302
3.2.1	Thin-Walled Vessel - Illustrative Example	D-303
4.0	Experimental Justification for Technical Approach	D-401
5.0	References and Charts	D-501

USE FOR TV, EWITTEN MATERIAL ONLY

Appendix D

List of Figures

<u>Figure No.</u>		<u>Page</u>
D-1	Estimate of Cyclic Life of a Thick Walled Vessel	D-503
D-2	Cyclic History of a Thick Walled Vessel	D-503
D-3	Prediction of Cyclic Life of a Thick Walled Vessel	D-504
D-4	Schematic of Sustained & Cyclic Flow Growth	D-505
D-5	Combined Sustained & Cyclic Stress Life Data	D-505
D-6	Schematic Representation of Thin Walled Vessel Life	D-506
D-7	Flow Growth Rate Curve	D-507
D-8	Determination of Initial and Critical Flow Sizes	D-507
D-9a	Stress Intensity Magnification Factors for Deep Surface Flows	D-508
D-9b	Critical Flow Size Curves at LOX Temp - 2219-T87 Aluminum	D-508
D-10	Arithmetic Integration of Flow Growth Rate Data	D-509
D-11	Cyclic Flow Growth Rates	D-509
D-12	Prediction of Cyclic Life of a Thin Walled Vessel	D-510
D-13	Stress Intensity vs Cycles to Failure Correlation For Various Stress Levels	D-511
D-14	Stress Intensity vs Cycles to Failure Correlation For 2219-T87 Aluminum at Room Temperature	D-512
D-15	Stress Intensity vs Cycles to Failure Correlation For 2219-T87 Aluminum at -320°F	D-512

USE FOR TYPEWRITTEN MATERIAL ONLY

APPENDIX D - FRACTURE MECHANICS ASSESSMENT

1.0 INTRODUCTION

1.1 APPLICATION TO SAFETY ANALYSES

One of the more hazardous elements in many systems is the subsystem under pressure. The fragmentation hazard of components under pressure is especially difficult to analyze because little is understood about the physical law governing the failure process. Improved accuracy of the predictions of the time or cycles to failure can reduce the risk of equipment damage and personnel injury. The following sections describe a model of fracture mechanics which has been validated by experimental results. Use of this model in safety analyses will help to reduce risk levels associated with pressurized systems.

1.2 DISCUSSION OF ANALYSIS METHOD

1.2.1 Symbols

A list of symbols used in the mathematical model is included herein. Detailed descriptions of methods and derivations may be found in the references listed in Section 5.0.

LIST OF SYMBOLS

K_I	Plane strain stress intensity factor.
K_{Ii}	Plane strain stress intensity factor at initial conditions.
K_{Ic}	Plane strain critical stress intensity factor or fracture toughness of the material.
K_{TH}	Plane strain threshold stress intensity level.
a	Semi-minor axis of the ellipse $\frac{x^2}{c^2} + \frac{y^2}{a^2} = 1$ or crack depth
$2c$	Crack length of the semi-elliptical surface flaw.
t	Thickness of plate (specimen).
ϕ	Complete elliptical integral of the second kind having modulus k defined as $k = (1 - a^2/c^2)^{1/2}$
σ	Uniform stress applied at infinity and perpendicular to the plane of crack.
σ_{op}	Maximum design operating stress.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.2.1 (Continued)

- σ_{ult} Ultimate strength of the material.
- σ_{ys} Uniaxial tensile yield strength of the material.
- Q Flaw shape parameter $= \phi^2 - 0.212 (\sigma/\sigma_{ys})^2$.
- M_K Stress intensity magnification factor for deep surface flaws based on Kobayashi's solution.
- α Proof test factor $= 1/(K_{I1}/K_{Ic})$.
- N Number of cycles.
- T_j Time
- R Ratio of minimum to maximum stress during a cycle.

Subscripts

- cr at critical conditions
- i at initial condition
- op operational

1.2.2 General

The minimum operational cyclic life of a pressure vessel at the maximum design operating stress can be determined if the proof test factor α , maximum design operating stress σ_{op} , fracture toughness K_{Ic} , and the experimental cyclic and sustained stress² flaw growth for the vessel materials are available. Proof test factor with σ_{op} and K_{Ic} establishes the initial and critical flaw size. For the cycles with the short hold times at the maximum pressure, the cyclic flaw growth data alone is sufficient to predict the number of cycles required to grow from the initial to the critical flaw size. If the vessel is to be pressure cycled with the prolonged hold times at the maximum pressure, the cyclic as well as sustained stress flaw growth data are needed. The minimum remaining cyclic life of the vessel, in this case, is the number of cycles required to reach the threshold stress intensity K_{TH} . Knowing the applied and anticipated pressure cycle history of the vessel, the minimum remaining cyclic life of the pressure vessel at σ_{op} can be predicted and the assessment of the vessel can be made with regard to the fracture mode. This is discussed in detail in the following sections.

Section 2.0 deals with the prediction of the cyclic life of a thick-walled vessel while the thin-walled vessel is treated in Section 3.0. Section 4.0 gives the experimental justification for the technical approach taken in Sections 2.0 and 3.0.

2.0 PREDICTION OF CYCLIC LIFE FOR A THICK-WALLED VESSEL

Prediction of the cyclic life of a thick-walled pressure vessel can be made utilizing the proof test factor and the relations between K_{I1}/K_{Ic} and cycles to failure for various values of R (ratio of the minimum to maximum stress during a cycle) for the material-environment combination. This can best be illustrated by an example.

Suppose a liquid nitrogen 5Al-2.5Sn(ELI) titanium pressure vessel is successfully proof tested with LN_2 to a factor of 1.25 X the maximum design operating pressure. For illustration purposes, it is assumed that the proof tested tank is subjected to the following pressure cycles before and during the flight. It is also assumed that all the cycles are applied with R equal to zero.

1. 240 loading cycles with the maximum stress as 90 percent of σ_{op} .
2. 70 loading cycles with the maximum stress as 95 percent of σ_{op} .
3. A long duration flight cycle at σ_{op} .

It is desired to assess the structural integrity of the pressure vessel from the fracture mechanics viewpoint.

The combined sustained and cyclic stress life curve for 5Al-2.5Sn(ELI)Ti at -320°F is reproduced from Reference 8 in Figure D1. Since the vessel is proof tested with $\phi = 1.25$, the maximum possible K_{I1}/K_{Ic} ratio that could exist in the vessel after the proof test at σ_{op} would be 0.80. This is shown by Point A in Figure D1. Hence, at 90 percent of σ_{op} , K_{I1}/K_{Ic} is 0.72. The 240 loading cycles of 0.90 σ_{op} as the maximum stress change the K_{I1}/K_{Ic} ratio from Point A to Point B. Point B is 240 cycles to the left of Point A, with the cycles measured along the abscissa of the plot. Hence, the K_{I1}/K_{Ic} ratio at the end of 240 cycles at 0.9 σ_{op} is 0.778.

The stress is increased by 5 percent after the end of 240 cycles at 0.90 σ_{op} . The flaw size remains the same during the stress increase. Therefore, the K_{I1}/K_{Ic} ratio at the beginning of 70 cycles at 0.95 σ_{op} is $(0.95/0.90) \times 0.778 = 0.821$. This is shown by Point B in Figure D1.

The 70 cycles at 0.95 σ_{op} change the K_{I1}/K_{Ic} ratio from Point B to Point C where Point C is 70 cycles to the left of Point B in Figure D1. K_{I1}/K_{Ic} ratio at the end of 70 cycles at 0.95 σ_{op} is 0.85. Hence, K_{I1}/K_{Ic} ratio based on σ_{op} is $(1.0/0.95) \times 0.855 = 0.895$.

The threshold stress intensity value for sustained stress flaw growth for the material under LN_2 environment is 90 percent of K_{Ic} (8). Since at the beginning of the long duration flight cycle the K_{I1}/K_{Ic} ratio is less than K_{TH}/K_{Ic} , the vessel is considered to be safe for the flight. Also, it can be seen from Figure D1 that 10 cycles at σ_{op} will raise K_{I1}/K_{Ic} to the level of K_{TH}/K_{Ic} . Hence, the estimated minimum remaining cyclic life for the vessel is 9 (10 - a long duration flight cycle) cycles.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 (Continued)

This is the procedure followed in assessing the structural integrity of the thick-walled vessels. In the first analysis for the assessment of the structural integrity of the thick-walled vessel, it is always assumed that all the pressure cycles are applied at $R = 0$. Since the analysis based on $R = 0$ will always show the remaining cyclic life less than that based on the analysis of $R \neq 0$ (actual R ratios), the prediction of cyclic life based on the analysis of $R = 0$ is invariably conservative. If the pressure vessel is shown unsatisfactory for the flight based on $R = 0$, then prediction analysis for the remaining cyclic life is conducted based on the actual R values at which the cycles are applied. For clarity purposes, an illustrative example is given below.

Suppose a thick-walled 6Al-4V(STA) titanium helium tank is successfully proof tested at a proof test factor of 1.50 X the maximum design operating stress. Suppose the proof tested tank is subjected to the following pressure cycles before the flight, which is also shown in Figure D2.

1. 200 loading cycles with the maximum stress as 90 percent of σ_{op} and $R = 0.1$. Environment is Room Temperature (R.T.).
2. 4300 loading cycles with the maximum stress as σ_{op} and $R = 0.7$ - R.T.
3. 260 loading cycles with the maximum stress as 95 percent of σ_{op} and $R = 0.4$ R.T.
4. 40 loading cycles with the maximum stress as σ_{op} and $R = 0.1$ R.T.

The cyclic life curves for 6Al-4V(STA) titanium for the environment of R.T. air are reproduced for $R = 0.0$, $R = 0.1$, $R = 0.4$, and $R = 0.7$ from Reference (10) in Figure D3. The difference between the plots of cyclic life against K_{II}/K_{IC} for $R = 0$ and $R = 0.1$ is negligible for this material-environment combination, and hence both are shown by the same plot in Figure D3. The threshold stress intensity level for the material in the environment of R.T. air is 90 percent of K_{IC} (10).

The maximum possible K_{II}/K_{IC} ratio that could exist in the vessel after the proof test at σ_{op} is $1/\sqrt{2} = 0.667$. From Figure D3, it can be seen from $R = 0$ plot that the maximum cycles to failure is about 600 at σ_{op} if the hold times at maximum stress are small. If the analysis is based on $R = 0$ instead of actual R , the pressure-cycle history shows that the vessel is critical. In the following, the assessment of the vessel is made based on the appropriate values of R .

At the beginning of 200 loading cycles with the maximum stress as $0.90 \sigma_{op}$, the maximum K_{II}/K_{IC} is given by $0.90 \times 0.667 = 0.60$. This point is indicated by E on $R = 0.1$ curve. The 200 loading cycles of $0.90 \sigma_{op}$ and $R = 0.1$ change the K_{II}/K_{IC} ratio from Point E to Point D on the plot of $R = 0.1$. The K_{II}/K_{IC} ratio at the end of 200 loading cycles of $R = 0.1$ is 0.63.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 (Continued)

The stress is increased by 10 percent at the end of 200 cycles. Hence, the K_{Ii}/K_{Ic} ratio at the beginning of 4300 cycles at σ_{op} and $R = 0.7$ is $(1.0/0.9) \times 0.63 = 0.70$. This is shown by Point D on the plot of $R = 0.7$. The 4300 loading cycles at σ_{op} and $R = 0.7$ change the K_{Ii}/K_{Ic} ratio from Point D to Point C on the plot of $R = 0.7$ where its value is 0.78.

The stress is decreased by 5 percent at the end of 4300 cycles. Hence, the K_{Ii}/K_{Ic} ratio at the beginning of 260 cycles at $0.95 \sigma_{op}$ is $(0.95/1.0) \times 0.78 = 0.74$ which is shown by Point C on $R = 0.4$ plot. The 260 cycles at $0.95 \sigma_{op}$ and $R = 0.4$ change K_{Ii}/K_{Ic} ratio from Point C to Point B on $R = 0.4$ where its value is 0.80.

The stress is increased by 5 percent at the end of 260 cycles. Hence, the K_{Ii}/K_{Ic} ratio at the beginning of 40 cycles at σ_{op} is $(1.0/0.95) \times .80 = 0.84$ which is illustrated by Point B on $R = 0.1$ plot. The 40 cycles at σ_{op} and $R = 0.1$ increases K_{Ii}/K_{Ic} ratio from 0.84 to 0.875 which is shown by Point A in Figure D3.

Since the stress intensity at the end of 40 cycles at σ_{op} is less than the threshold stress intensity, the vessel is considered to be safe for the flight. It will take 20 loading cycles at σ_{op} and $R = 0.1$ to increase K_{Ii}/K_{Ic} from 0.875 to 0.90. Thus, the estimated minimum cyclic life remaining for the vessel is 20 cycles.

USE FOR TYPEWRITTEN MATERIAL ONLY

3.0. PREDICTION OF CYCLIC LIFE FOR A THIN-WALLED VESSEL**3.1 BACKGROUND**

Analysis for the prediction of the cyclic life for a thin-walled vessel is somewhat different than that for the thick-walled vessel. The flaw depth becomes deep with respect to the wall thickness prior to reaching the critical size for the thin-walled vessels. The stress intensity factor calculated by the Kobayashi equation for the deep flaw is higher than the one predicted by the original Irwin equation for the shallow surface flaw. As a result, the subcritical flaw-growth rates for the thin-walled vessels, having the same flaw size and subjected to the same stress as the thick-walled vessels, are higher than those for the thick-walled vessels. Thus, the total cyclic life for a thin-walled vessel is shorter than that determined from curves of the type shown in Figure D4 and D5, that are developed from the data of specimens where a_{cr}/t is less than 0.5. If data similar to that in Figures D4 and D5 (K_{Ii}/K_{Ic} against cycles to failure and K_{Ii}/K_{Ic} versus time to failure) can be developed from the specimens having deep flaws and the comparable thickness as that of the vessel, then the analysis described in Section 2.0 can be used to predict the cyclic life of the thin-walled vessel remaining after the proof test. This data development is complicated and expensive since the stress intensity magnification factor for deep surface flaws, M_K , is the function of a/t as well as $a/2c$. (Variation of σ/σ_{ys} has a smaller effect on M_K than the variations of a/t .) Consequently, a large number of specimens would be required to sort out the effect of a/t and $a/2c$. In the absence of these data, the following analysis is used to calculate the cyclic life. The main assumptions involved in the analysis are:

1. In the thin-walled vessels, the flaws are long with respect to their depth and consequently, Q is assumed to be equal to unity in the Kobayashi equation. This, in turn, raises stress intensity and hence the flaw growth rates and gives the lower bound of the cyclic life.
2. The flaw growth rates are dependent on K_{Ii}/K_{Ic} and hence, flaw growth rates obtained from the specimens where a_{cr}/t is less than 0.5 can be used for the specimens where a_{cr}/t approaches unity.
3. It is assumed that below the threshold level, flaw growth rates are not affected by the presence of the propellant. Consequently, the flaw growth rates for the material-propellant temperature combination are simulated by the material-temperature combination.

To determine the cyclic life of a thin-walled tank, the following relations are required:

1. The proof test factor, σ_{op} , K_{Ic} and K_{TH} .
2. σ versus " a " curve, similar to Figure D6, for K_{Ic} and K_{TH} to determine the flaw sizes a_i , a_{cr} , and a_{TH} . The σ versus " a " curve can be obtained from the following equation:

3.1 (Continued)

$$\sigma = K_{I1}/(1.1 M_K \sqrt{\pi a})$$

3. K_{I1}/K_{Ic} versus flaw growth rate da/dN curve to determine flaw growth rate at any stress intensity level.

The flaw growth rates can be obtained by differentiating the K_{I1}/K_{Ic} versus cycles to failure curve, similar to that of Figure D5. This curve is obtained from the specimens where a_{cr}/t is less than half. For an assumed maximum cyclic stress level, say σ_1 , the given K_{I1}/K_{Ic} versus N curve can be converted to an a/Q versus N curve by the equation:

$$a/Q = \frac{1}{1.21 \pi} \left(\frac{K_{I1}}{\sigma_1} \right)^2$$

The slope of a/Q versus N curve gives the plot for the flaw growth rate d/dN (a/Q) versus K_{I1}/K_{Ic} for the stress level σ_1 .

From the above equation for a given K_{I1} , a/Q at the stress level σ_2 is related with a/Q at σ_1 as:

$$(a/Q)_{\sigma_2} = \left(\frac{\sigma_1}{\sigma_2} \right)^2 \left(\frac{a}{Q} \right)_{\sigma_1}$$

From this equation, it can be concluded that the flaw growth rate at any stress level σ_2 is related to the growth rate at σ_1 as follows:

$$(d/dN (a/Q))_{\sigma_2} = \left(\frac{\sigma_1}{\sigma_2} \right)^2 (d/dN (a/Q))_{\sigma_1}$$

This stress level effect is supported by the experimental data in References (7), (8), (10), and (11). If the basic K_{I1}/K_{Ic} versus cycle data is obtained from the experimental tests where the specimens are cycled at a maximum stress at or near the expected operating stress levels in the vessel, the effect of stress level need not be considered. The flaw growth rate obtained in this manner from Figure 7 for 5Al-2.5Sn(EL1) titanium for the maximum cyclic stress level of 139 ksi is given in Figure D7. Also, as pointed out by Tiffany, et al (7), flaw growth rates can be approximated by measuring striation spacings on electron fractographs obtained from the fracture face of a surface flawed specimen cycled to failure in tension.

3.2 APPROACH

Knowing the proof stress and K_{Ic} , the maximum possible flaw size that can exist at σ_{proof} (after the proof test assuming rapid depressurization) can be determined from the plot of σ against "a" for K_{Ic} . This flaw size is denoted by a_1 in the illustrative example of Figure D3. Also knowing σ_{op} and K_{Ic} , the maximum possible flaw size that can exist at σ_{op} can be determined from the same plot for K_{Ic} . This flaw size is shown by a_{cr} in Figure D3. Similarly, the maximum flaw size that could exist at σ_{op} and the threshold stress intensity K_{IH} is shown by a_{TH} .

USE FOR TYPEWRITTEN MATERIAL ONLY

3.2 (Continued)

If the cycles to be applied to the vessel have short hold times at the maximum stress σ_{op} , then the stress intensity at σ_{op} can be allowed to reach the critical value K_{Ic} . In this case, the flaw growth rates for the vessel are arithmetically integrated using the stress intensity magnification values from Figure D9a to calculate the number of cycles required to grow from a_i to a_{cr} . The relatively simple procedure for this integration is illustrated in Figure D10. If a_{cr} is less than the wall thickness, then the total estimated cycles to failure will be obtained, and if it exceeds the wall thickness then the total estimated cycles to leak will be obtained as explained in Section 2.4.2, (5). The effect of deep flow stress intensity magnification on predicted critical flaw sizes for a typical tank material is shown in Figure D9b, for both thick and thin-walled vessels.

If the cycles to be applied to the vessel have long hold times at the maximum stress, the stress intensity could not be allowed to exceed the sustained stress threshold value K_{TH} . In this case, the flaw growth rates are arithmetically integrated using M_K to calculate the number of cycles required to grow from a_i to a_{TH} . This is the procedure followed in the prediction of the cyclic life in Volumes II and III of (5).

The prediction of the remaining cyclic life and the structural integrity of the thin-walled vessel can best be demonstrated by an illustrative example.

3.2.1 Thin-Walled Vessel - Illustrative Example

Suppose a thin-walled 6A1-4V titanium (STA) propellant tank containing N_2O_4 at R.T. is successfully proof tested with water at R.T. to a proof test factor of 1.41 x the maximum design operating stress, σ_{op} . Suppose the proof tested tank is subjected to the following pressure cycles before the flight.

1. 20 loading cycles with the maximum stress as 90 percent of σ_{op} .
2. 12 loading cycles with the maximum stress as 95 percent of σ_{op} .
3. 5 loading cycles with the maximum stress as σ_{op} .

It is desired to assess the structural integrity of the pressure vessel from the fracture mechanics standpoint and estimate the minimum cyclic life remaining for the vessel at σ_{op} . This example is treated with specific numbers since the stress intensity factor has to be corrected for a/t ration according to Figure D9a. The thickness of the tank is 0.022". The maximum design operating stress, σ_{op} , is 87.5 KSI. The material of this gage under the above-mentioned environmental conditions has the minimum fracture toughness of 37 ksi \sqrt{in} and the threshold stress intensity of 60 percent of K_{Ic} .

The σ versus "a" plots are given for K_{Ic} and $K_{TH} = 0.80 K_{Ic}$ in Figure D8. Since proof stress is 1.41 x $\sigma_{op} = 123.6$ KSI, it is clear from Figure D8 that the maximum possible a_i that could exist is 0.0143". Here it is assumed that the depressurization from the proof pressure is rapid enough so that no significant flaw growth occurs during the depressurization. Also, as shown in Figure D8, for the stress level of σ_{op} , a_{cr} is 0.0196" and a_{TH} is 0.0160".

USE FOR TYPEWRITTEN MATERIAL ONLY

3.2.1 (Continued)

The plot of K_{I1}/K_{Ic} versus flaw growth rate for 6Al-4V titanium at R.T. is reproduced in Figure D11 for $\sigma = 100$ ksi from Reference 10. The 99% confidence level flaw growth rate curve is used in the calculation of cyclic life. Since the above flaw growth rate curve is obtained from the cyclic data of $R = 0.0$, it is assumed in this example that all the cycles are applied at $R = 0.0$.

Taking the effect of stress level on the flaw growth rates into account, flaw growth rates are arithmetically integrated from $a_i = 0.0143$ " to $a_{cr} = 0.0196$ " according to Figure D10 to calculate the cycles to failure for the stress level of σ_{op} . The plot of flaw depth against cycles to failure for the stress level of σ_{op} is shown in Figure D12.

When the maximum cyclic stress is $0.95 \sigma_{op}$, a_i is still 0.0143 " but a_{cr} is 0.0208 " and $a_{TH} = 0.0167$ " from Figure D8. Based on the stress level of $0.95 \sigma_{op}$, the flaw growth rates are integrated from $a_i = 0.0143$ " to $a_{cr} = 0.0208$ " to calculate the cycles to failure. Similar procedure is followed to obtain the relation of flaw depth against cycles to failure for the stress level of $0.90 \sigma_{op}$. These plots are shown in Figure D12.

At the end of the proof cycle and the beginning of the first cycle at the maximum cyclic stress of $0.90 \sigma_{op}$, the maximum possible flaw depth is 0.0143 ". This is shown by Point D in Figure D12. The 20 loading cycles with the maximum stress as $0.90 \sigma_{op}$ change "A" from Point D to Point C on the plot of $0.90 \sigma_{op}$ as shown in Figure D12.

The tank wall stress is increased by 5 percent at the end of 20 loading cycles with the maximum stress as $0.90 \sigma_{op}$. The flaw size remains the same during the stress increase. This is shown by Point C on the plot of $0.95 \sigma_{op}$ in Figure D12.

The 12 loading cycles with the maximum stress as $0.95 \sigma_{op}$ change "A" from Point C to Point B on the plot of $0.95 \sigma_{op}$ in Figure D12.

At the end of 12 loading cycles with the maximum stress as $0.95 \sigma_{op}$, the stress is increased by 5 percent. This is shown by Point B on the plot of σ_{op} in Figure D12.

The 5 loading cycles with the maximum stress as σ_{op} change "a" from Point B to Point A on the plot of σ_{op} in Figure D12. The flaw depth at A is 0.01534 ". This is smaller than a_{TH} which is 0.0160 ". Hence the vessel is considered to be safe for the flight. Also from Figure D12, it will take 7 cycles at σ_{op} , to increase the flaw depth from 0.01534 " to 0.0160 ". Hence, the minimum estimated cyclic life remaining for the vessel is 7 cycles.

4.0 EXPERIMENTAL JUSTIFICATION FOR TECHNICAL APPROACH

The technical approach taken in Sections 2.0 and 3.0 would need the justification in the following areas:

1. Representation of cyclic life with K_{I1}/K_{Ic} .

It has been shown (6, 7, 9, 10, 11) that the cyclic life of surface flawed specimens correlates well with the maximum initial stress intensity K_{I1} at the tip of the surface flaw. Also in Reference 10, large number of surface flawed specimens of the same thickness are cycled to failure at four different stress levels ranging from 96 ksi to 126 ksi. The results, K_{I1}/K_{Ic} against cycles to failure, are cited in Figure D13. This shows that for a given K_{I1}/K_{Ic} , the stress level has little real influence on the cyclic life.

2. Use of uniaxial specimen data in the prediction of the cyclic life of biaxially loaded pressure vessel.

The cyclic life data obtained from the preflawed 5Al-2.5Sn(EL1) titanium tank tests agree very well with the corresponding cyclic life data obtained from preflawed uniaxial test specimens at R.T., -320°F, and -423°F temperatures (7).

The same reference also shows that cyclic life data obtained from 2219-T87 aluminum tank tests at R.T. and -320°F temperature correlate very well with those obtained from uniaxial specimens. The stress intensity versus cycles to failure correlations for 2219-T87 aluminum specimens and tanks at R.T. and -320°F are recited from Reference 7 in Figures D14 and D15. Similar correlation is shown for Ladish D6A-C steel at R.T. in Reference (6). These results indicate that the uniaxial plane strain cyclic life data and flaw growth rates can be applied directly to the prediction of the cyclic lives and flaw growth rates of the biaxially loaded pressure vessels where the flaws grow under plane strain conditions.

USE FOR TYPEWRITTEN MATERIAL ONLY

5.0 REFERENCES AND CHARTS

The following references will provide the analyst with more detail regarding the use of fracture mechanics models in predicting vessel life and safety factors for design and use.

1. E. T. Wessel, W. G. Clark and W. K. Wilson, "Engineering Methods for the Design and Selection of Materials Against Fracture," U.S. Army Tank and Automotive Center Report, Contract No. DA-30-069-AMC-602(T), 1966.
2. Fracture Toughness Testing and Its Applications, A.S.T.M. Spec. Tech. Publication No. 381, 1965.
3. A. S. Kobayashi, "On the Magnification Factors of Deep Surface Flaws," Structural Development Research Memorandum No. 16, The Boeing Company, December 1965.
4. F. W. Smith, "Stress Intensity Factor for a Semi-Elliptical Flaw," Structural Development Research Memorandum No. 17, The Boeing Company, August 1966.
5. C. F. Tiffany, J. M. Masters, and R. C. Shah, "Fracture Mechanics Assessment of Apollo Launch Vehicle and Spacecraft Pressure Vessels"-Volume 1. The Boeing Company Document Number D2-114248-1, November 1968.
6. C. F. Tiffany and P. M. Lorenz, "An Investigation of Low-Cycle Fatigue Failures Using Applied Fracture Mechanics," ML-TDR-64-53, May 1964.
7. C. F. Tiffany, P. M. Lorenz and R. Hall, "Investigation of Plane Strain Flaw Growth in Thick-Walled Tanks," NASA CR-54837, February 1966.
8. C. F. Tiffany, P. M. Lorenz and R. Hall, "Extended Loading of Cryogenic Tanks," NASA CR-72252, 1966.
9. C. F. Tiffany and J. N. Masters, "Investigation of the Flaw Growth Characteristics of 6Al-4V Titanium Used in Apollo Spacecraft Pressure Vessels," NASA CR-65586, March 1967.
10. J. N. Masters, "Cyclic and Sustained Load Flaw Growth Characteristics of 6Al-4V Titanium," NASA CR-92231, July 1968.
11. L. R. Hall, "Plain Strain Cyclic Flaw Growth in 2014-T62 Aluminum and 6Al-4V (ELI) Titanium," NASA Report for Contract N00033-7993, To Be Published in November 1968.
12. R. P. Wei, "Some Aspects of Environment -- Enhanced Fatigue Crack Growth," presented at A.S.T.M. Fall Meeting in Atlanta, Ga., October 3, 1968.

USE FOR TYPEWRITTEN MATERIAL ONLY

5.0 (Continued)

13. J. E. Srawley and J. B. Esgar, "Investigation of Hydrotest Failure of Thiokol Chemical Corporation 260-inch Diameter SL-1 Motor Case," NASA TMX-1194, January 1966.
14. A.S.T.M. Special Committee on Fracture Testing of High-Strength Metallic Materials, "Progress in the Measurement of Fracture Toughness and the Application of Fracture Mechanics to Engineering Problems," Materials Research and Standards, Volume 4, No. 3, March 1964.
15. C. F. Tiffany, "Investigation of Preflawn 2219 Aluminum Tanks", Boeing Document D5-13663, August 1966.
16. S. V. Glorioso, et al., "Lunar Module Pressure Vessel Operating Criteria Specification," SE-V-0024, NASA/MSO, October 1968.
17. P. M. Lorenz, "Fracture Toughness and Subcritical Flaw Growth Characteristics of Inconel 718 in the Environment of Pressurized Hydrogen," Boeing Document D2-114404-1, December 1968.
18. W. E. Witzell, "Fracture Data for Materials at Cryogenic Temperatures," Technical Report AFML-TR-67-257, November 1967.
19. C. F. Tiffany and F. A. Pall, "An Approach to the Prediction of Pressure Vessel Minimum Fatigue Life Based Upon Applied Fracture Mechanics," Boeing Document D2-22437, March 1963.
20. W. Haese, C. Summers and D. Crensey, "Titanium and Stainless Steel SI-C Helium Bottle Investigation," Boeing Document D5-10057-1, December 1964.
21. F. A. Pall, "Plane Strain Fracture Toughness of Cryogenic Tankage Materials," Boeing Document D2-22567.
22. C. M. Carman, D. F. Armento and H. Markus, "Plane Strain Fracture Toughness of High Strength Aluminum Alloys," Journal of Basic Engineering, December 1965.
23. L. R. Hall, "Plane-Strain Cyclic Flaw Growth of 2014-T62 Aluminum and 6Al-4V(ELI) Titanium," NASA CR-72473, December

USE FOR TYPEWRITTEN MATERIAL ONLY

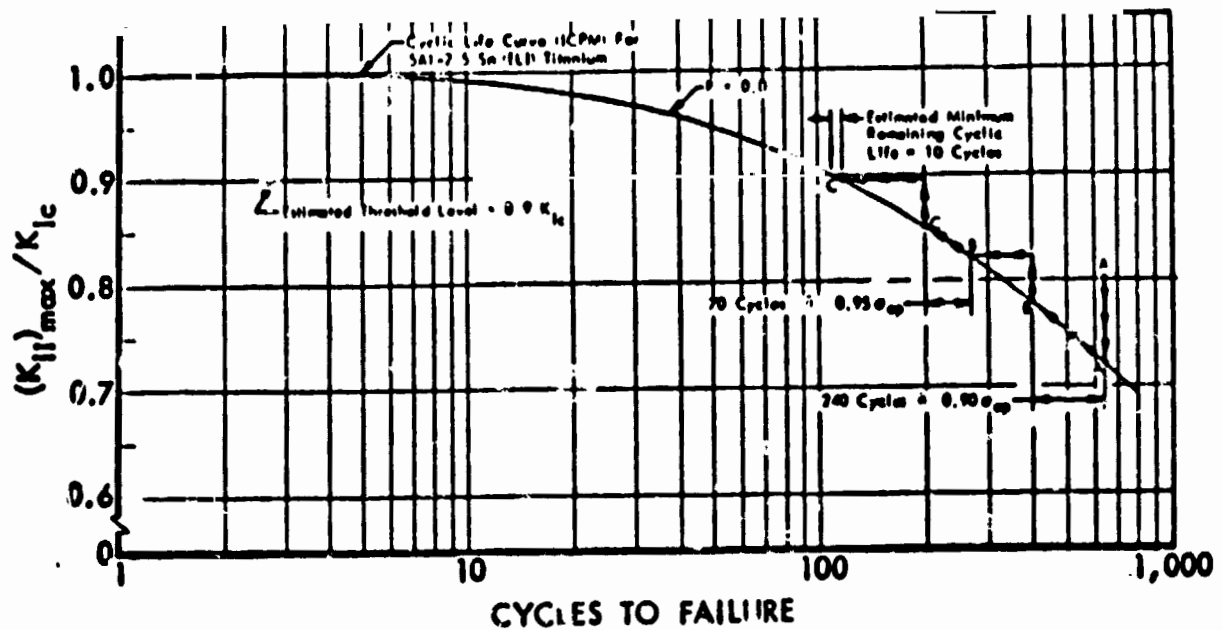


Figure D1: ESTIMATION OF CYCLIC LIFE OF A THICK WALLED VESSEL
BASED ON $R = 0$ (Illustrative Example)

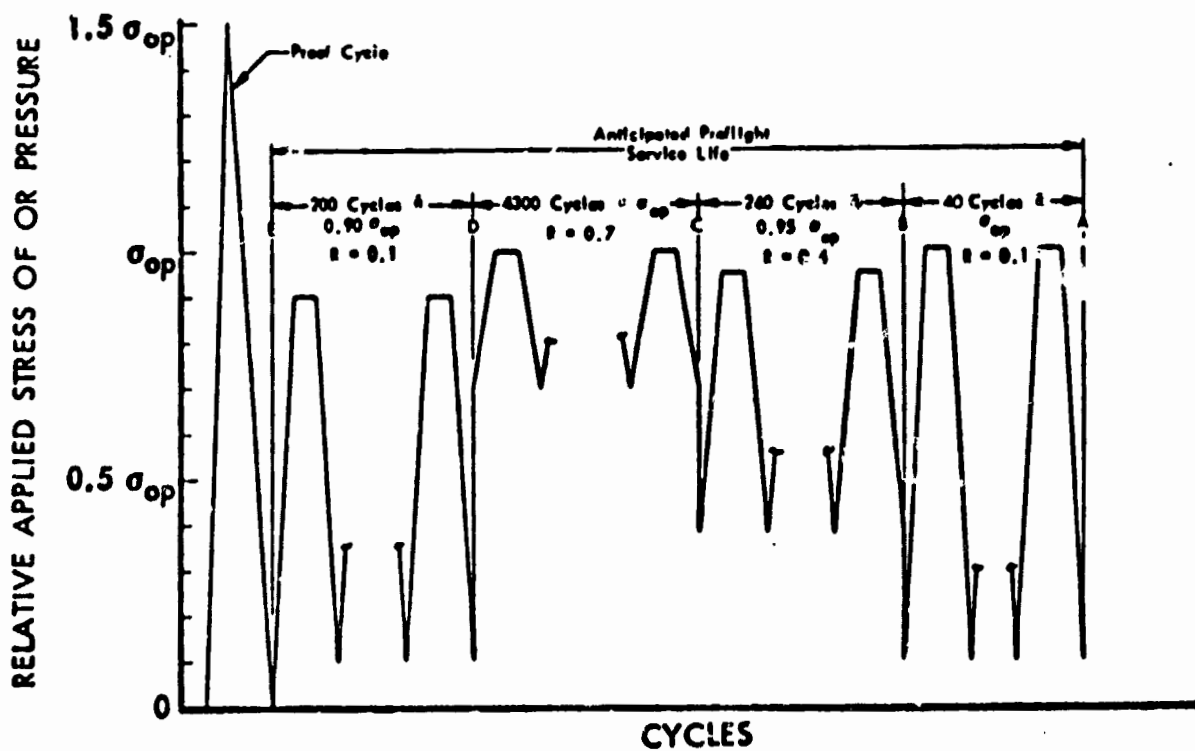


Figure D2: CYCLIC HISTORY OF A THICK WALLED VESSEL
(Illustrative Example)

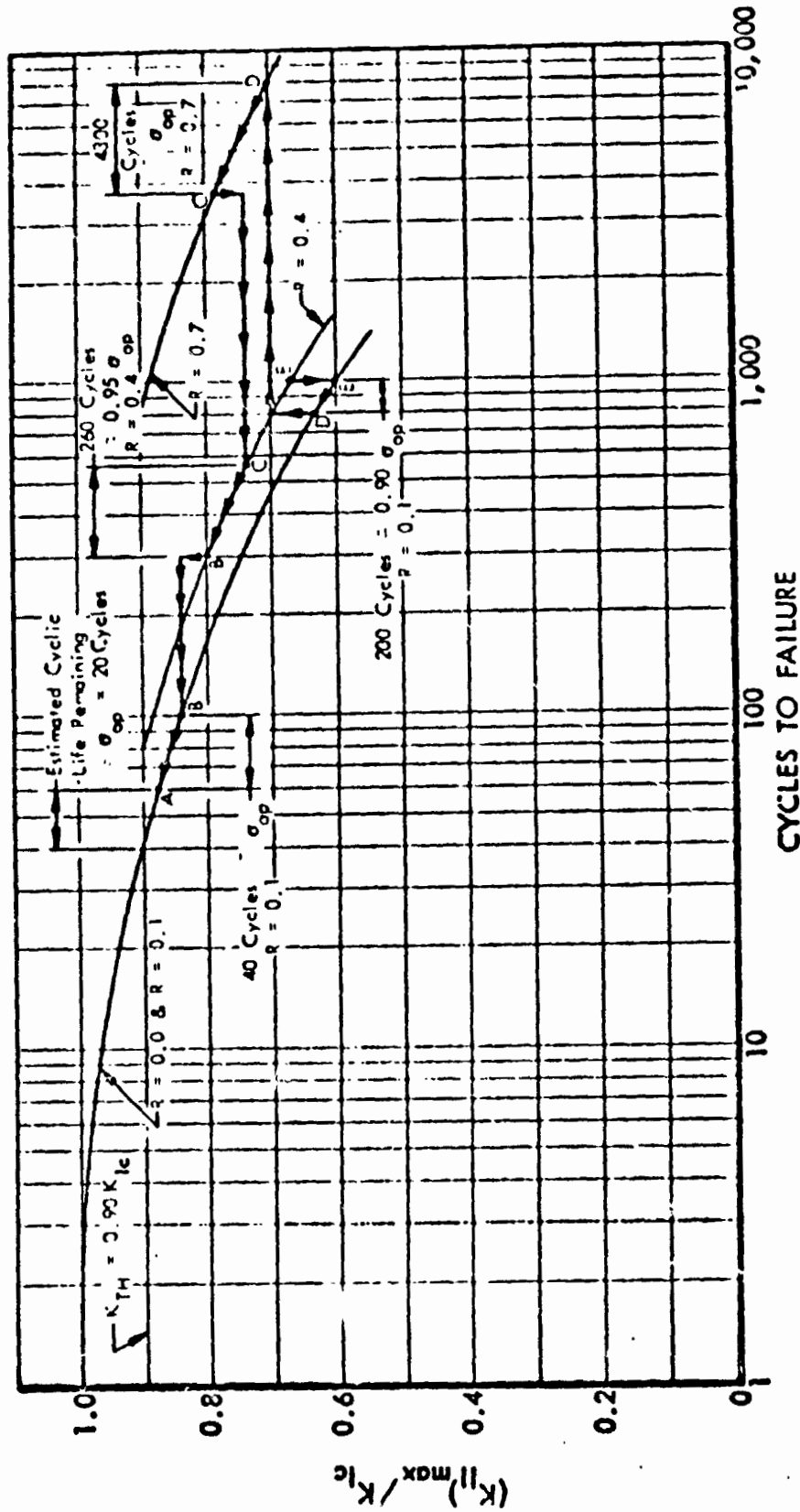


Figure D3: PREDICTION OF CYCLIC LIFE OF A THICK WALLED VESSEL
(Illustrative Example)

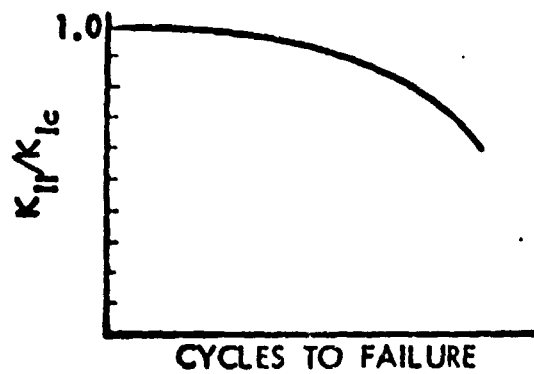


Figure D4 A

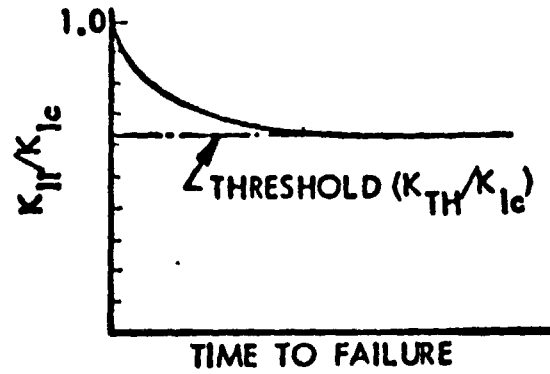


Figure D4 B

Figure D4 SCHEMATIC OF SUSTAINED & CYCLIC FLAW GROWTH

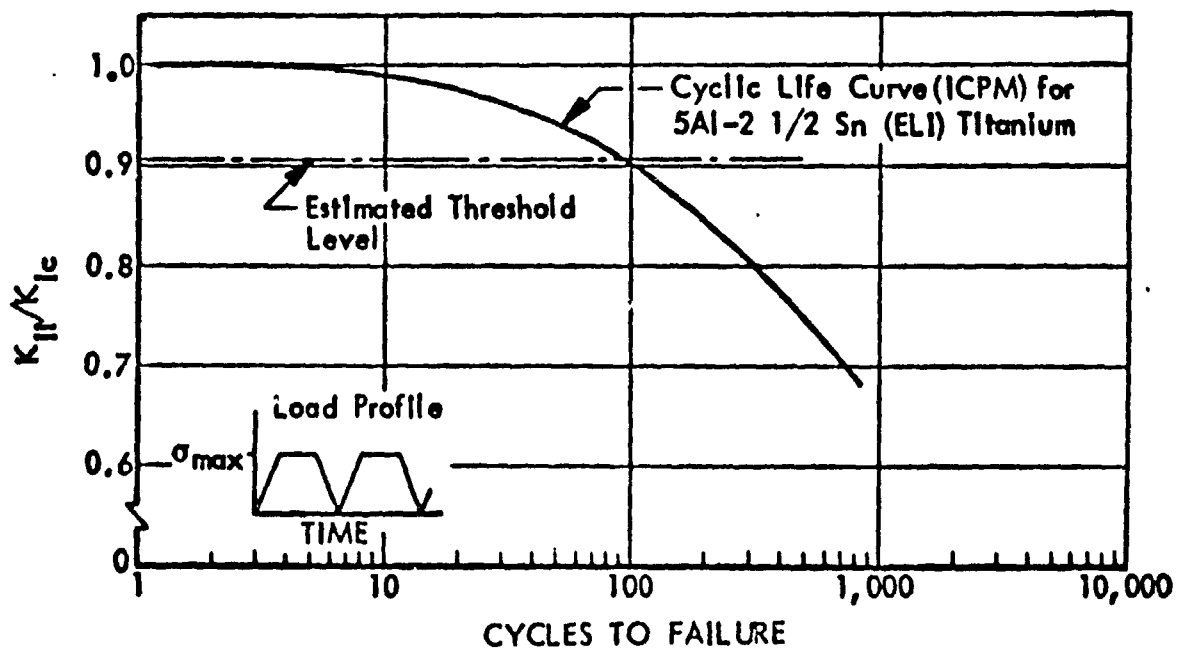


Figure D5: COMBINED SUSTAINED & CYCLIC STRESS LIFE DATA (5Al-2 1/2 Sn (ELI) Titanium @ -320°F)

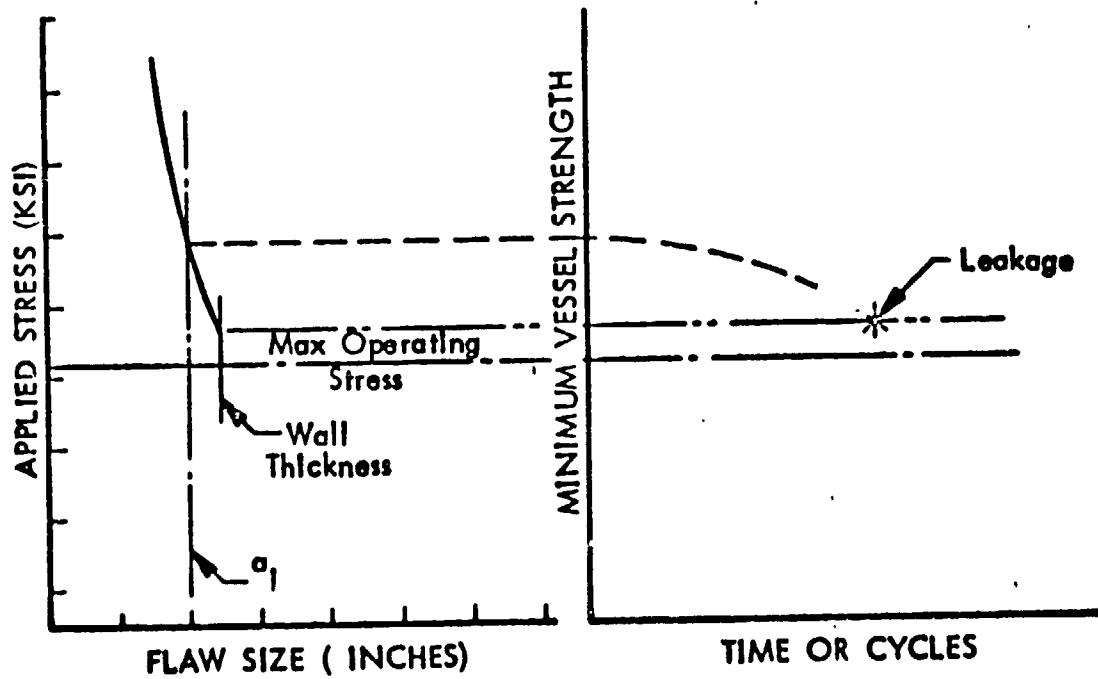
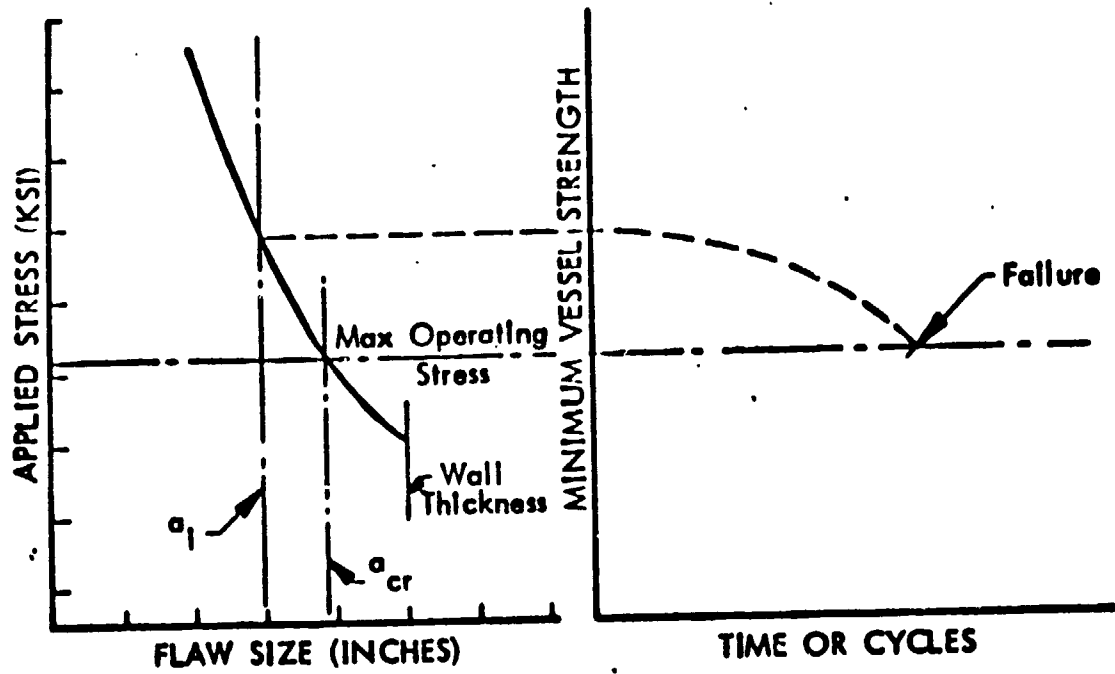


Figure D6. SCHEMATIC REPRESENTATION OF THIN WALLED VESSEL LIFE

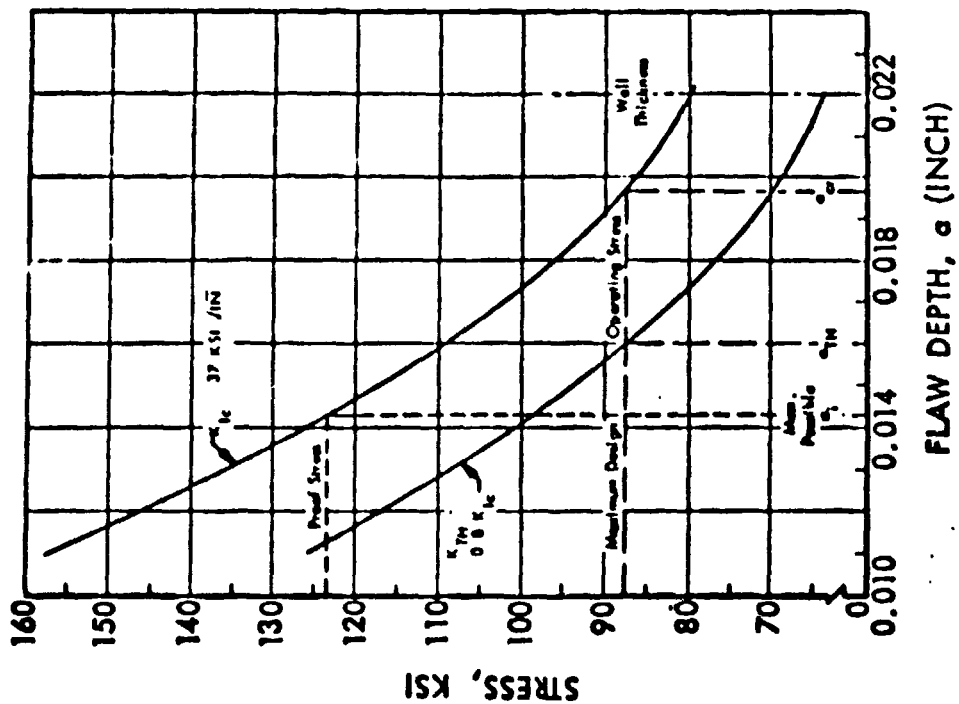


Figure D8: DETERMINATION OF INITIAL AND CRITICAL FLAW SIZES

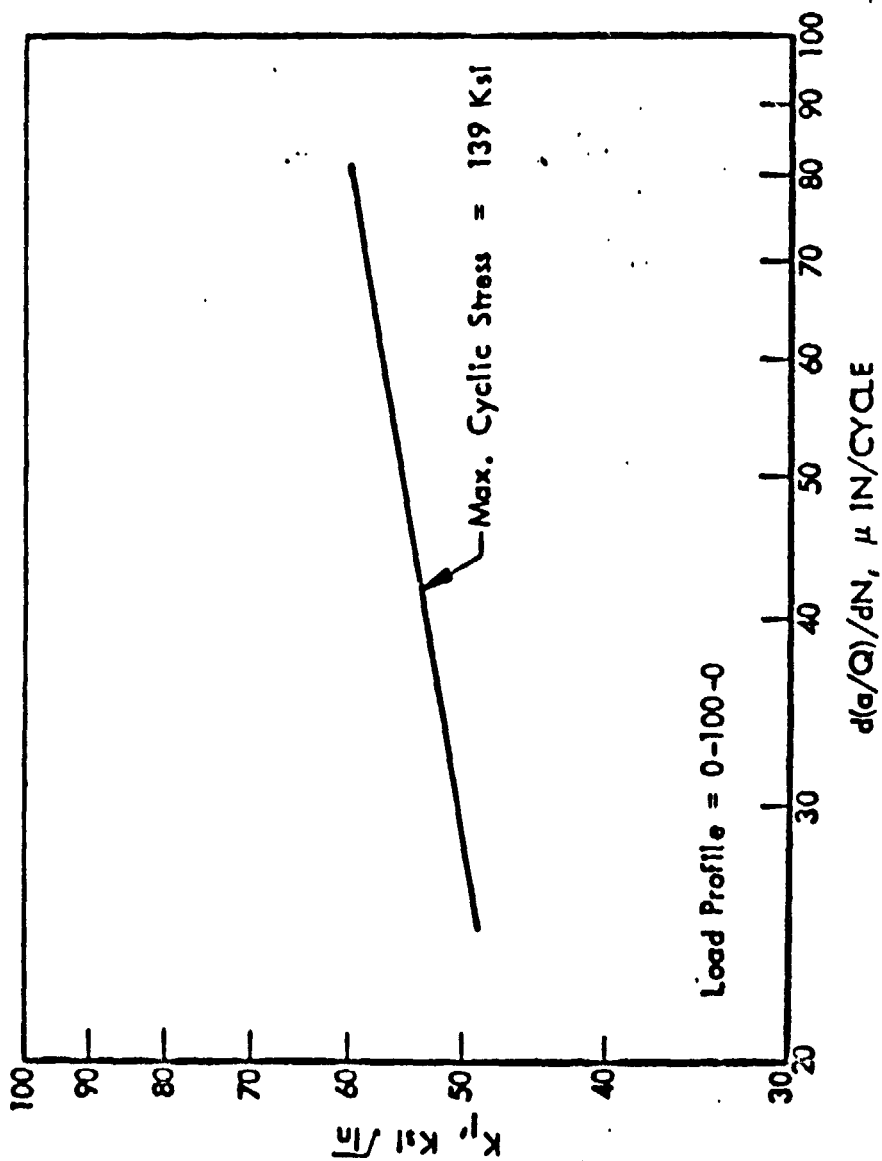


Figure D7: FLAW GROWTH RATE CURVE (5A1-2 1/2Sn (ELI) TITANIUM @ -320°F)

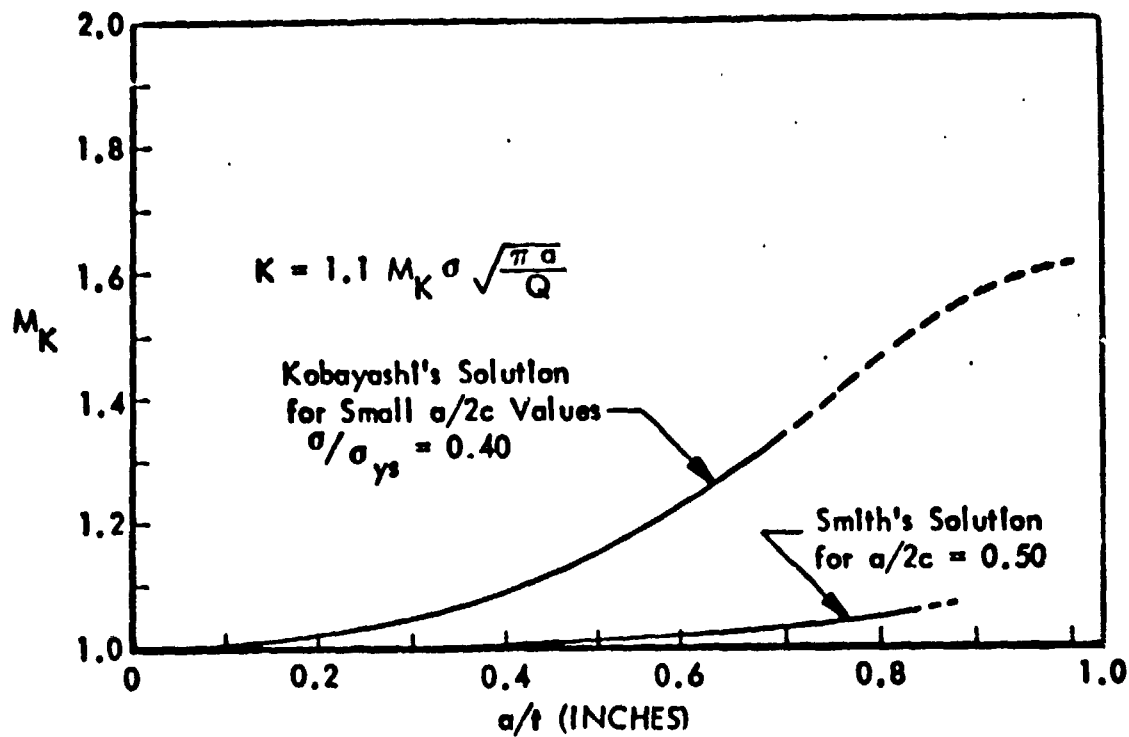


Figure D9a. STRESS INTENSITY MAGNIFICATION FACTORS FOR DEEP SURFACE FLAWS

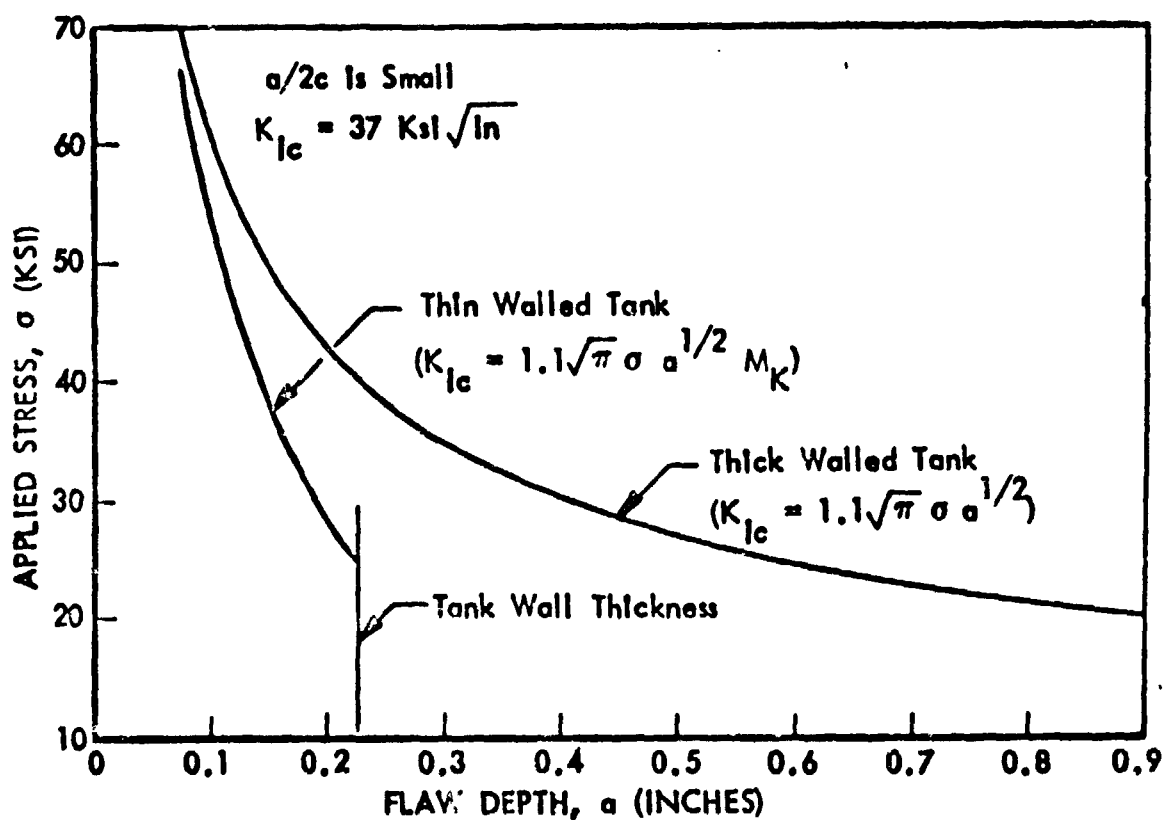
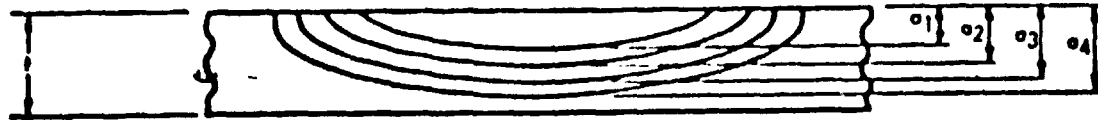


Figure D9b. CRITICAL FLAW SIZE CURVES @ LOX TEMPERATURE 2219-T87 ALUMINUM



a	Δa	a/t	M_K	K	MEAN K	MEAN da/dN	ΔN	N
a_1	$a_2 - a_1$	a_1/t	M_{K1}	K_1	$\frac{K_1 + K_2}{2}$	da_{1-2}/dN	ΔN_1	ΔN_1
a_2	$a_3 - a_2$	a_2/t	M_{K2}	K_2	$\frac{K_2 + K_3}{2}$	da_{2-3}/dN	ΔN_2	$\Delta N_1 + \Delta N_2$
a_3								$\Delta N_1 + \Delta N_2 + \Delta N_3$

1 Obtain From Kobayashi's Solution Of M_K vs a/t

2 $K = 1.1\sqrt{\pi} \sigma(a)^{1/2} M_K$

3 Obtain From Basic K vs da/dN Curve

Figure D10: ARITHMETIC INTEGRATION OF FLAW GROWTH RATE DATA
(Deep Flaws In Thin Walled Vessels)

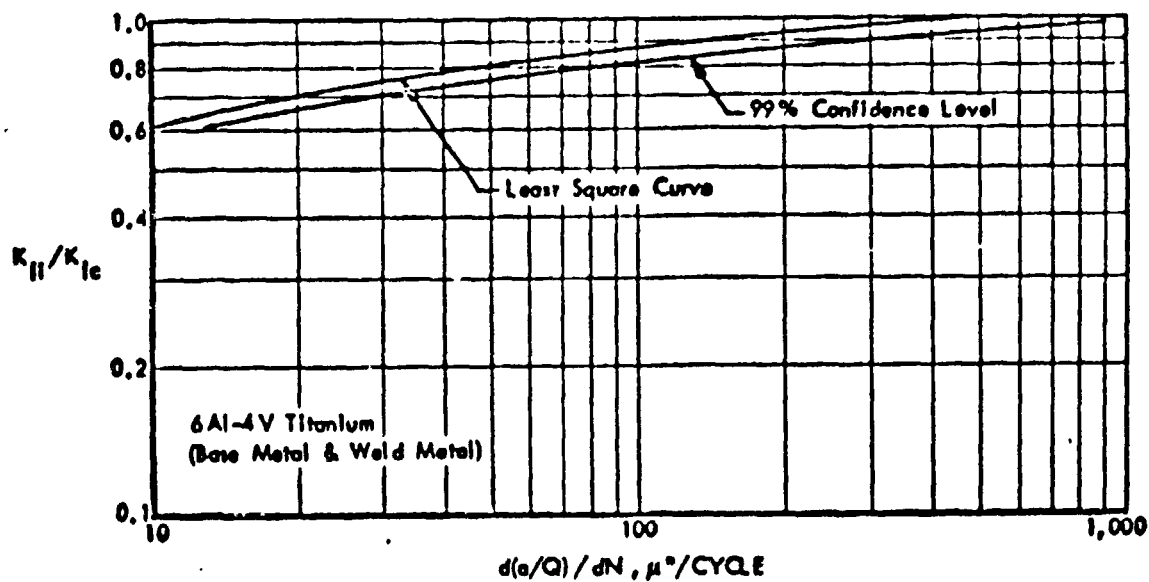
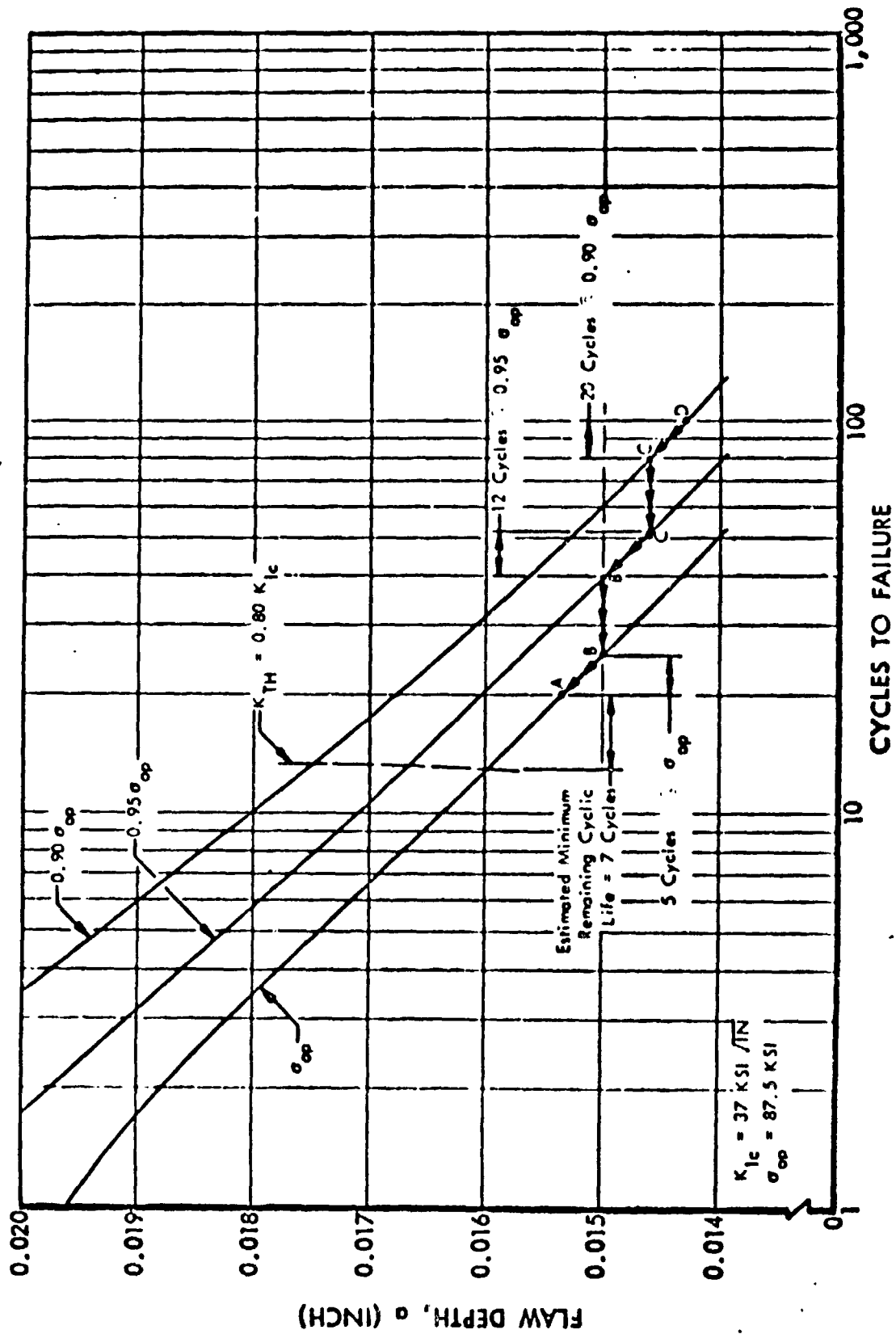
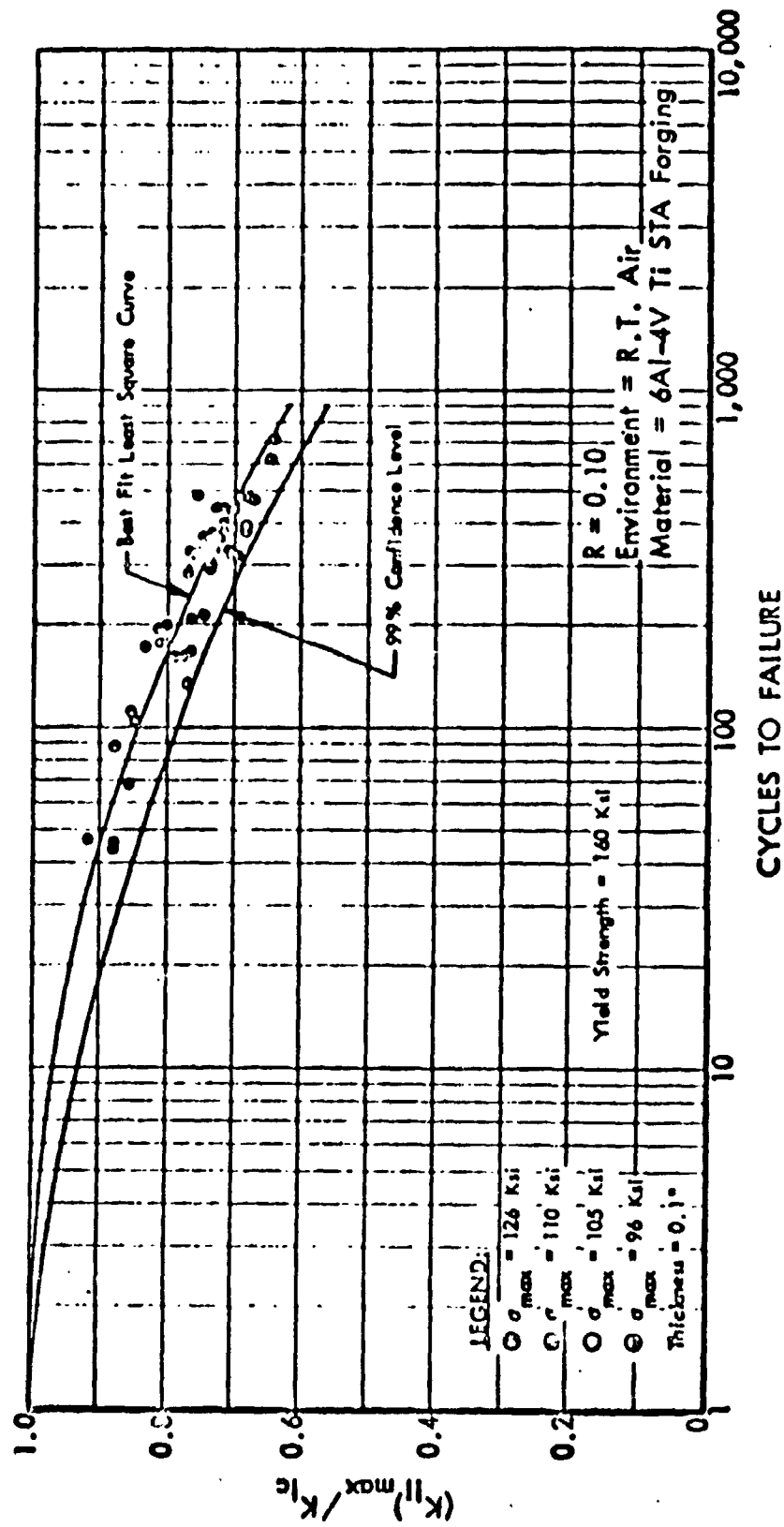


Figure D11 CYCLIC FLAW GROWTH RATES
(For $\sigma_{max} = 100$ Ksi)





FigureD13: STRESS INTENSITY VS. CYCLES TO FAILURE CORRELATION FOR VARIOUS STRESS LEVELS

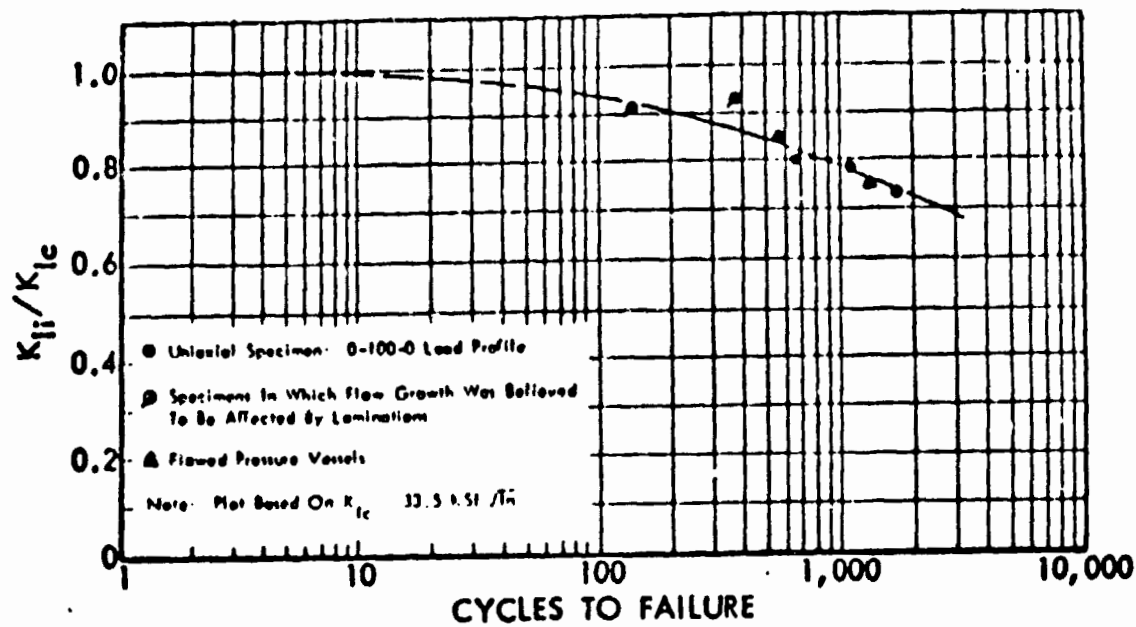


Figure D14: STRESS INTENSITY VS. CYCLES TO FAILURE CORRELATION FOR 2219-T87 ALUMINUM AT ROOM TEMPERATURE

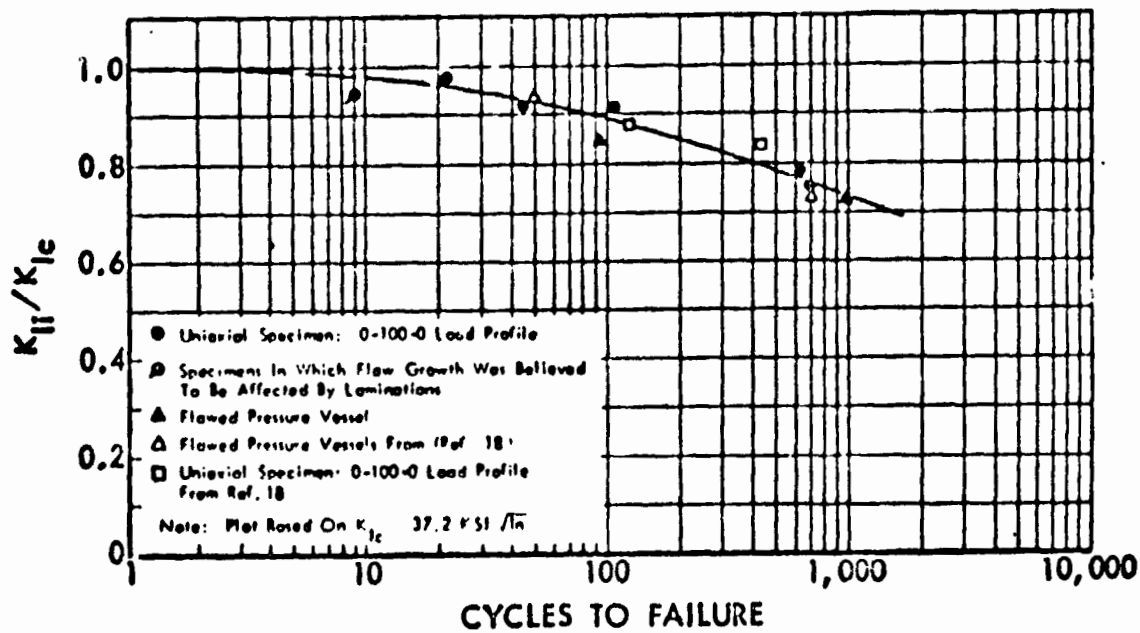


Figure D15 STRESS INTENSITY VS. CYCLES TO FAILURE CORRELATION FOR 2219-T87 ALUMINUM AT -320 °F

Appendix E

<u>Paragraph</u>	<u>FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS Contents</u>	<u>Page</u>
	List of Figures	E-003
1.0	Introduction	E-101
1.1	Application to Safety Analysis	E-101
1.2	References	E-101
1.3	Summary Description of FMECA	E-101
1.3.1	Definition of FMECA	E-101
1.3.2	Objectives of Conducting FMECA	E-102
1.3.3	Application of the FMECA Method	E-102
1.3.4	Procedure of FMECA	E-103
2.0	Procedure for Failure Mode and Effects Analysis	E-201
2.1	System Definition	E-201
2.1.1	Accomplishment	E-201
2.1.2	Input Documentation	E-202
2.1.2.1	System Technical Development Plans	E-202
2.1.2.2	Trade-Off Study Reports	E-202
2.1.2.3	System Description and Specifications	E-203
2.1.2.4	Equipment Design and Drawings	E-203
2.1.2.5	Coding Systems	E-203
2.1.2.6	Test Results	E-203

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix E (Continued)

	<u>Contents</u>	<u>Page</u>
2.2	Logic Block Diagram	E-203
2.3	Failure Mode and Effects Analysis	E-205
3.0	Procedures for Criticality Analysis	E-301
3.1	Criticality Procedure	E-301
3.2	Critical Failure Mode Identification	E-301
3.3	Criticality Number Calculation	E-302
3.3.1	C _r Calculation Example	E-304
3.3.2	Format for C _r Calculation	E-304
4.0	Summary of FMECA and CA	E-401
4.1	Preparation of FMECA Summary	E-401
4.2	Criticality List	E-402

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix E
List of Figures

<u>Figure No.</u>		<u>Page</u>
E-1	General FMEA Logic Block Diagram Scheme	E-204
E-2	General Format for Failure Mode and Effects Analysis	E-208
E-3	General Format for Criticality Number Calculation	E-306
E-4	General FMECA Summary Format	E-403

USE FOR TYPEWRITTEN MATERIAL ONLY

Appendix E

FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS

1.0 INTRODUCTION

1.1 APPLICATION TO SAFETY ANALYSIS

Failure Mode, Effects, and Criticality Analyses (FMECA) have been used for years as a method of determining the reliability of a system. The same method may be used to determine the degree of safety to be expected from a system. The adaptation of the FMECA to system safety analysis requires that a different perspective be adopted by the analyst. The goal of a reliability analysis is the prevention of "loss of mission", "loss of system", and "system function degradation". The goal of a system safety analysis is the prevention of "death or injury of personnel", "damage of the system", and "system safety degradation". These system safety goals are achieved by considering every component failure mode, including improper commands to the component, which may have potentially damaging effects. A list of components which are critical to safe system use may be derived from the analysis, and the criticality (or probability of causing personnel injury or system damage) calculated for the appropriate failure modes.

1.2 REFERENCES

The material in this appendix has been chiefly extracted from Procedures For Failure Mode, Effects, And Criticality Analysis (FMECA), document number RA-0060013-1A, Office of Manned Space Flight, National Aeronautics And Space Administration, August 1966. Information on application of the FMECA method is also found in Procedure for Performing Systems Design Analysis, Drawing No. 10M30111, Revision A, George C. Marshall Space Flight Center, NASA, June 1964; and in Reliability Stress And Failure Rate Data For Electronic Equipment, MIL-HDBK-217A, Bureau of Naval Weapons, Department Of Defense, December 1965.

1.3 SUMMARY DESCRIPTION OF FMECA

1.3.1 Definition Of FMECA

For system safety analyses, FMECA is a procedure which documents all possible failures in a system design within specified ground rules, determines failure mode analysis, the effect of each failure on system operation, identifies single failure points critical to safety, and ranks each failure according to criticality category of failure effect and probability of occurrence. The total analysis

USE FOR TYPEWRITTEN MATERIAL ONLY

1.3.1 (Continued)

is conducted in two steps: The Failure Mode and Effect Analysis (FMEA), and the Criticality Analysis. It has been found most practical to assume that the effects of each failure studied during the analysis are not negated by the occurrence of a benign failure.

1.3.2 Objectives of Conducting FMECA

The FMEA is accomplished to provide:

- a. The design engineer with a method of selecting a design with a high probability of safe operation,
- b. Early visibility of system interface problems,
- c. Identification of single failure points critical to system safety,
- d. Early criteria for test planning,
- e. Quantitative and uniformly formatted data input to the system safety prediction, assessment, or other safety study.

1.3.3 Application Of The FMECA Method

An FMECA should be initiated as an integral part of the early design phase of system functional assemblies. If a Gross Hazards Analysis has been conducted, the results can be used to guide the development of the FMECA. Subsystems which the Gross Hazards Analysis has indicated are most hazardous can be developed first in the logic diagram for the failure mode and effects study. An FMECA should be performed at the highest system level feasible. This facilitates a safety criticality ranking of all of the major system elements so the FMECA effort can be allocated to those elements which are most determinant upon overall safety.

Proposed design changes can be incorporated in the analysis, and the effect on system safety can be predicted. Changes which are proposed to enhance safety should be considered from all aspects to ensure that the modification is cost effective and that the state-of-the-art is reflected in the new design.

FMECA, like all analytical tools, can be conducted on completed systems. The increased cost of modifying a physical system is a major determining factor for safety improvements. As a result, the improvements recommended for completed systems must be very cost effective. Therefore, it is incumbent on the analyst to be as accurate as possible in the prediction of safety improvements so that safety costs can be fairly evaluated.

USE FOR TYPEWRITTEN MATERIAL ONLY

1.3.4 Procedure of FMECA

FMECA is performed in two phases: (1) Failure Mode and Effects Analysis (FMEA), and (2) Criticality Analysis (CA). The combination of these two phases provides (3) Failure Mode Effects and Criticality Analysis (FMECA). Section 2 provides procedures for FMEA; Section 3 provides procedures for CA; and Section 4 combines the FMEA and CA into the FMECA.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.0 PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS

2.1 SYSTEM DEFINITION

2.1.1 Accomplishment

Accomplishment of an FMEA on a system consists of the following general steps:

- a. Obtain all descriptive information available on the system to be analyzed. This should include such documents as functional block diagrams, system descriptions, specifications, drawings, system component identification coding, operational profiles, environmental profiles, and reports bearing on reliability and safety such as feasibility or reliability studies of the system being analyzed and of past similar systems.
- b. Construct a logic block diagram of the system to be analyzed, similar to that shown in Figure E-1, for each equipment configuration involved in the system's use.

The diagrams are developed starting at the top level of the system and extending downward to the lowest level of system definition at the time of analysis. These logic block diagrams are not descriptive block diagrams of the system that show the interconnection of equipments. The logic block diagrams used for an FMEA show the functional interdependencies between the system components so that the effects of a functional failure may be readily traced through the system.

All redundancies or other means for preventing failure effects should be shown as functional blocks or notes.

Where certain functions are not required in an operational time phase, the information may be shown by a dotted block as in the case of component 0.5 in Figure E-1 or by other suitable means.

- c. At the lowest level of system definition, as developed from the top down, analyze each failure mode of the system component and its effect on the system. Where system functional definition has not reached the level of identification of the system functions with the specific type of hardware that will perform these functions, the FMEA should be based upon failure of the system functions giving the general type of hardware envisioned as the basis for system design.

Four basic conditions of component or functional failure should be considered:

- 1) Premature operation
- 2) Failure to operate at a prescribed time

USE FOR TYPEWRITTEN MATERIAL ONLY

2.1.1 (Continued)

- 3) Failure to cease operation at a prescribed time
- 4) Failure during operation.

The FMEA assumes that only the failure under consideration has occurred. When redundancy or other means have been provided in the system to prevent undesired effects of a particular failure, the redundant element is considered operational and the failure effects terminate at this point in the system. When the effects of a failure propagate to the top level of a system and cause the system to fail, the failure is defined as a critical failure in the system.

When an FMEA is being performed on a system which is already built, the analyst may find cases where redundancies or other means of preventing failure effects do little to improve the failure situation or where the redundancies may actually worsen it. These cases should be reported for the next higher level. Where the scope of the FMEA program permits, the redundancy or other failure effects preventive means should not halt the continuation of the failure effects analysis toward the top level of the system.

- d. Document each potential failure mode of each system component and the effects of each failure mode on the system by completing an FMEA format similar to that shown in Figure E-2. Instructions for filling out the FMEA format are given in Section 2.3.

2.1.2 Input Documentation

The following documentation is representative of the information required for system definition and analysis:

2.1.2.1 System Technical Development Plans

To define what constitutes and contributes to the various types of system failure, the technical development plans for the system should be studied. The plans will normally state the system objectives and specify design requirements for operations, maintenance, test, and activation. Detailed information in the plans will normally provide a mission or operational profile and a functional flow block diagram showing the gross functions that the system must perform. Time diagrams and charts used to describe system functional sequence will aid the analyst to determine the time feasibility of various means of failure detection and correction in the operating system. Also required is a definition of the operational and environmental stresses that the system is expected to undergo and a list of the acceptable conditions of functional failure under these stresses.

2.1.2.2 Trade-Off Study Reports

To determine the possible and more probable failure modes and causes in the system, trade-off study reports should identify the areas of marginal design and should explain the design compromises and operating conditions agreed upon.

USE FOR TYPEWRITTEN MATERIAL ONLY

2.1.2.3 System Description and Specifications

The descriptions and specifications of the system's internal and interface functions, starting at the highest system level and progressing to the lowest level of system development to be analyzed, are required for construction of the FMEA logic block diagrams. A logic block diagram as used in the FMEA and as described in Paragraph 2.1.1.b shows the functional interdependence within the system and permits the effects of a failure to be traced. System descriptions and specifications usually include either or both functional and equipment block diagrams that facilitate the construction of the logic block diagrams required for the FMEA. In addition, the system descriptions and specifications give the limits of acceptable performance under specified operating and environmental conditions.

2.1.2.4 Equipment Design Data and Drawings

Equipment design data and drawings identify the equipment configuration performing each of the system functions.

Where functions shown on a FMEA functional block diagram depend on a replaceable module in the system, a separate FMEA may be performed on the internal functions of the module. The effects of possible component failure modes in the module on module inputs and outputs then describe the failure modes of the module when it is viewed as a system component.

2.1.2.5 Coding Systems

For consistent identification of system functions and equipment, an approved coding system should be adhered to during the analysis. Use of coding systems common to the overall program are preferable.

2.1.2.6 Test Results

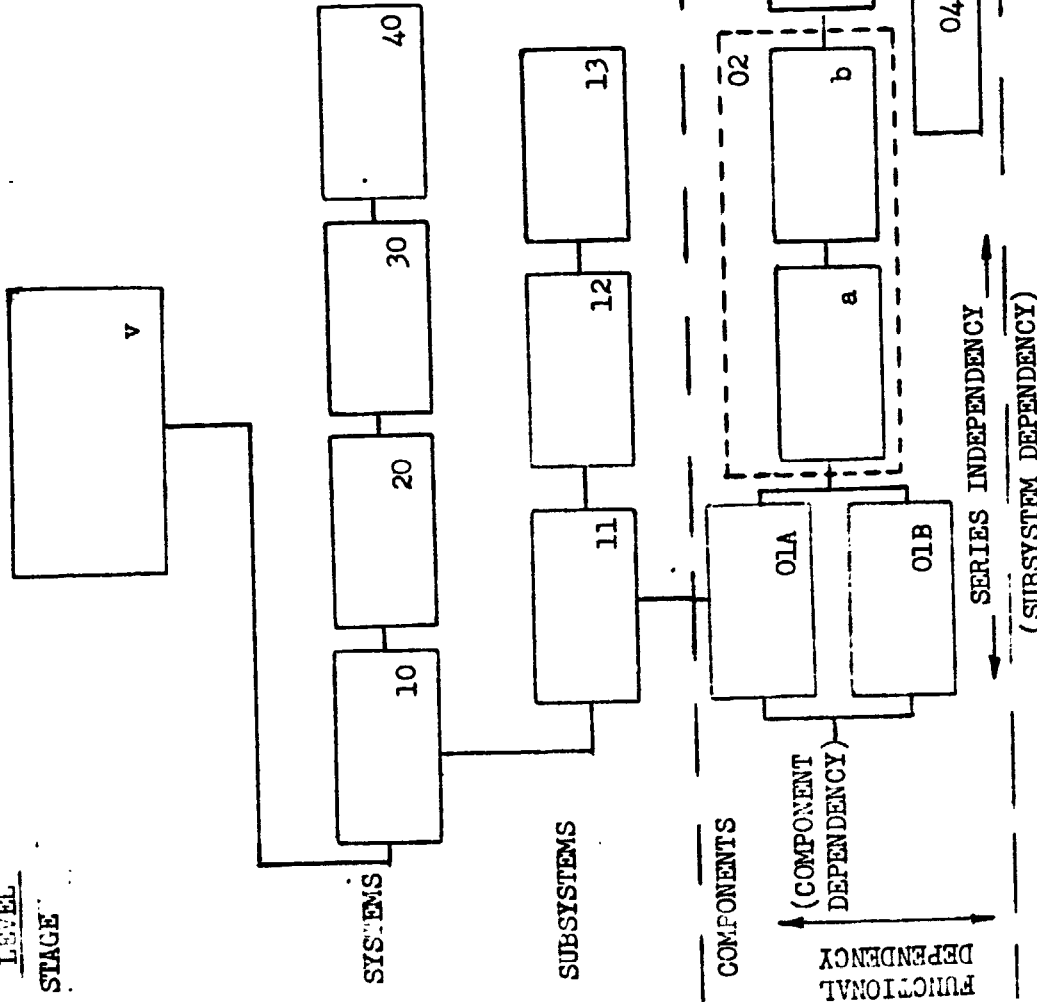
Tests run on the specific equipment under the identical conditions of use are desired. When such test data are not available, the analyst should collect and analyze the data obtained from studies and tests performed during current and past programs on equipment similar to those in the system and under similar use conditions.

2.2 LOGIC BLOCK DIAGRAM

The next step of the FMEA procedure is the construction of a logic block diagram of the system to be analyzed. The general reliability logic block diagram scheme for a system is shown in Figure E-1. This example system is for a space vehicle stage, and the notes given explain the functional dependencies of the stage components.

A system component at any level in the stage system may be treated as a system and may be diagrammed in like manner for failure mode and effects analysis. The results of the component's FMEA would define the failure modes critical to the component's operation, i.e., those that cause loss of component inputs or outputs. These failure modes will then be used to

LEVEL
STAGE



NOTES

1. Stage is dependent on 10, 20, 30 & 40; for the stage to operate, systems 10, 20, 30 & 40 must function.
2. System 10 is dependent on 11, 12 & 13; for the system to operate, subsystems 11, 12 & 13 must function.
3. Subsystem 11 is dependent on 01A, 01B, 02, 03, 05, 06, & 07; for the subsystem to operate, these components in series must function.
4. Components 01A & 01B are identical components, redundant for all failure modes unless otherwise indicated (See note 8).
5. Component 02 consists of two separable components a and b, but has only one part number.
6. Component 03 is functionally/operationally dependent on both component 04 and another subsystem.
7. Component 05 is not operational during flight.
8. Components 06 & 07 indicate standby safety circuit. Component 06 operates only when 07 fails in specified mode.

2.2 (Continued)

accomplish the FMEA at the next higher system level. This procedure ultimately leads to an FMEA for the stage, the space vehicle, and space system.

All system redundancies or other means for preventing failure effects are shown in the logic block diagram. This is because in single failure analysis, when a means exists to prevent the effects of a failure, the failure cannot be critical above the system level where the preventive means is effective.

2.3 FAILURE MODE AND EFFECTS ANALYSIS

The FMEA and its documentation are the next steps of the procedure. These are accomplished by completing the columns of an FMEA format similar to that given in Figure E-2 as follows:

<u>Column Number</u>	<u>Explanation or Description of Entries</u>
(1)	Name of system function or component under analysis for failure modes and effects. Breakdown of a system for analysis should normally be down to the lowest practicable level at the time of the FMEA. In special cases such as electronic systems using integral modular units as system building blocks, the modules may be listed rather than listing its parts.
(2)	Drawing number by which the contractor identifies and describes each component or module. These drawings should include configuration, mechanical, and electrical characteristics.
(3)	Reference designation used by manufacturer to identify the component or module on the schematic. Applicable schematic and wiring drawing numbers should also be listed.
(4)	Identification number of FMEA logic block diagram and of the function.
(5)	Concise statement of the function performed.
(6)	Give the specific failure mode after considering the four basic failure conditions: <ol style="list-style-type: none">1) Premature operation.2) Failure to operate at a prescribed time.3) Failure to cease operation at a prescribed time.4) Failure during operation.

For each applicable failure mode, describe the cause including operational and environmental stress factors if known.

2.3 (Continued)

Column
NumberExplanation or Description of Entries

- (7) Phase of mission in which critical failure occurs, e.g., Prelaunch: checkout, countdown; Flight: boost phase, earth orbit, translunar, lunar landing, etc. Where the subphase, event, or time can be defined from approved operational or flight profiles, the most definitive timing information should also be entered for the assumed time of critical failure occurrence. The most definitive time information that can be determined should also be given for the failure effects under the columns titled "Failure Effects On."
- (8) A brief statement describing the ultimate effect of the failure on the function or component being analyzed. Examples of such statements are component rendered useless, component's usefulness marginal, or structurally weakened to unacceptable reliability level. Timing information as described under (7) should be given.
- (9) A brief description of the effect of the failure on the next higher assembly. Timing information as described under (7) should be given as to time of failure effect.
- (10) A description of the effect of the component failure on the system. For the major systems of the overall space system, these effects are divided into failures affecting equipment safety and failures affecting personnel safety. Examples of failures affecting equipment safety are vehicle loss, stage damage, etc. Examples of failures affecting personnel safety are loss of crew, abort during flight, and loss of redundancy in safety systems. For lower level systems where effects on the overall space system are unknown, the effects of a failure on the system under analysis may be described as loss of system inputs or outputs. Examples of such effects are loss of signal output, loss of output pressure, and shorted power input. Timing information as described under (7) should be given.
- (11) A description of the methods by which the failure could be detected. Identify which of the following categories the failure detection means falls under:
- 1) On-board visual/audible warning devices.
 - 2) Automatic abort-sensing devices.
 - 3) Ground operational support system failure-sensing instrumentation.
 - 4) Flight telemetry, ground support equipment console display, etc.
 - 5) None

USE FOR TYPEWRITTEN MATERIAL ONLY

2.3 (Continued)

Column
NumberExplanation or Description of Entries

- (11) Contd. Timing information as described under (7) should be given with respect to the reaction time available between time of component failure, time of detection, and time of critical failure effect.
- (12) A description of what corrective actions that the flight crew and the ground crew could take to circumvent the failure. If applicable, the time available for effective action and the time required should be noted.
- (13) State the useful life of item under given environmental conditions.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

Page <u> </u> of <u> </u> Pages Date <u> </u> By <u> </u>		(13) Useful Life		
		(12) Corrective Action Time Available/Time Required		
		(11) Failure Detection Method		
		Failure Effect On	(10) System	
			(9) Subsystem	
			(8) Component/Functional Assembly	
		(7) Mission Phase		
(6) Failure Mode and Cause				
(5) Function				
Item Identification	(4) Reliability Logic Diagram Number			
	(3) Drawing Reference Designation			
	(2) Identification Number			
	(1) Name			

Figure E2 General Format For Failure Mode and Effects Analysis

3.0 PROCEDURES FOR CRITICALITY ANALYSIS

3.1 CRITICALITY PROCEDURE

The Criticality Analysis (CA) determines a system component's magnitude of criticality to system safety.

The CA is performed in two steps:

- a. Identify critical failure modes of all components in the FMEA for each equipment configuration in accordance with the categories listed in Paragraph 3.2. For FMEA's of lower level systems where the effect of failure modes on mission success or crew safety cannot be determined, the critical failure modes will be those that cause failure of one or more of the system's inputs or outputs.

The specific type of system failure is expressed as a unique loss statement. For major Apollo systems, example loss statements are crew loss, abort, and vehicle loss. For lower level systems, example loss statements are output signal loss, input power shorted, and loss of output pressure.

- b. Compute Critical Numbers (C_n) for each system component with critical failure modes. The method is given in Paragraph 3.3, and a format for the data is shown in Figure E-3.

The C_n for a system component is the number of system failures of a specific type expected per million missions due to the component's critical failures modes.

Where the factors involved in the calculation of system component criticality numbers vary with mission time, the mission is divided into mission phases such that the change in the factors are negligible during each phase. A criticality number is computed for each mission phase for a given loss statement.

The analyst responsible for the CA at the next higher system level continues the analysis using lower level CA's. Where the loss of an input or output of a lower level equipment is critical to equipment operational success at his system level, action should be taken to design the criticality out of the system or to reduce its criticality to an acceptable level by improvements in basic reliability, redundancy, or other means.

3.2 CRITICAL FAILURE MODE IDENTIFICATION

The first step of CA is the identification of critical failure modes from the FMEA's on the system.

3.2 (Continued)

Critical failure modes at higher levels in the overall space system should be identified according to approved nonambiguous loss statements. The following categories may be used:

HARDWARE CRITICALITY CATEGORIES :

- Category 1 - Hardware, failure of which results in loss of life of any crew member. This includes normally passive systems, i.e., emergency detection system, launch escape system, etc.
- Category 2 - Hardware, failure of which results in damage to the system but does not cause loss of life.
- Category 3 - Hardware, failure of which will not result in system damage nor cause loss of life.

At the lower system level where it is not possible to identify critical failure modes according to loss statements under the categories above, approved loss statements based upon loss of system inputs or outputs should be used (See Paragraph 3.1.a). Kennedy Space Center loss statements can be found in NASA Kennedy Space Center Publication KSC-STD-118(D), 3 February 1965, "Failure Effect Analysis of Ground Support Equipment". Marshall Space Flight Center loss statements can be found in NASA Marshall Space Flight Center Drawing No. 10M30111, Revision A, 26 June 1964, "Procedure for Performing Systems Design Analysis".

The loss statement used to identify a critical failure mode in a system should be prefixed with the word "actual", "Probable", "possible", or "none" which represents the analyst's judgment as to the conditional probability that the loss will occur given that the failure mode has occurred.

3.3 CRITICALITY NUMBER CALCULATION

The second step of the CA procedure is the calculation of Criticality Numbers (C_r) for the system components with critical failure modes.

A C_r for a system component is the number of system failures of a specific type expected per million missions due to the component's critical failure modes. The specific type of system failure is expressed by the critical failure mode loss statement discussed in Paragraph 3.2.

For a particular loss statement and mission phase, the C_r for a system component with critical failure modes is calculated with the following formula:

$$C_r = \sum_{n=1}^j (\beta \alpha K_E K_A \lambda_{GT} \cdot 10^6)_n \quad n = 1, 2, 3, \dots, j$$

USE FOR TYPEWRITTEN MATERIAL ONLY

3.3 (Continued)

where:

 C_T = Criticality number for the system component. j = Total number of critical failure modes in the system component under loss statement. β = Conditional probability that the failure effects of the critical failure mode occur given that the critical failure mode has occurred. α = Fraction of all failures (or λ_G) experienced by a component and that are due to the particular failure mode under consideration. K_E = Environmental factor which adjusts λ_G for difference between environmental stresses when λ_G was measured and the environmental stresses under which the component is going to be used. K_A = Operational factor which adjusts λ_G for the difference between operating stresses when λ_G was measured and the operating stresses under which the component is going to be used. λ_G = Generic failure rate of the component in failures per hour or cycle. t = Operating time in hours or number of operating cycles of the component. n = An index of summation for critical failure modes in the system component that fall under a particular loss statement.

The factor β is the probability of loss discussed in Paragraph 3.1, and should be limited to the following values:

<u>Failure Effects</u>	<u>Value of Beta</u>
Actual Loss	100 Percent
Probable Loss	Greater than 10 Percent to 100 Percent
Possible Loss	0 Percent to 10 Percent
None	0 Percent

The expression $(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)$ is the portion of C_T for the component due to one of its critical failure modes under a particular loss statement. After calculation of the part of C_T due to each of the component's critical failure modes under the loss statement, these parts are summed for all critical failure modes as indicated by:

USE FOR TYPEWRITTEN MATERIAL ONLY

3.3 (Continued)

$$\sum_{n=1}^1$$

A failure mode failure rate is represented in the formula for C_r by the product of the terms α , K_E , K_A , and λ_G . These terms should be replaced by actual failure mode failure rates determined from the test program as they become available. A sample calculation is given below.

3.3.1 C_r Calculation Example

For a given mission phase:

Given: System component with $\lambda_G = 0.05$ failures per 10^6 operating hours,

$$K_A = 10, \quad K_E = 50,$$

$\alpha = 0.30$ for one critical failure mode under loss statement, and

$\alpha = 0.20$ for the second critical failure mode under the same loss statement.

Let $\beta = 0.50$ and $t = 10$ hours.

Find: C_r for this system component during this mission phase.

Solution:

For the first critical failure mode; i.e., for $n = 1$

$$(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_1 = (0.50)(0.30)(50)(10)(0.05 \times 10^{-6})(10)(10^6) = 38$$

For the second critical failure mode; i.e., for $n = 2$

$$(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_2 = (0.50)(0.20)(50)(10)(0.05 \times 10^{-6})(10)(10^6) = 25$$

$j = 2$ and

$$C_r = \sum_{n=1}^2 (\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_n = 38 + 25 = 63$$

3.3.2 Format For C_r Calculation

The columns of the format for C_r calculations shown in Figure E-3 should be filled out as follows:

USE FOR TYPEWRITTEN MATERIAL ONLY

3.3.2 (Continued)

<u>Column Number</u>	<u>Explanation or Description of Entries</u>
(1) - (7)	These columns duplicate the information given in the same columns of the FMEA format shown in Figure E-2 and are explained in Paragraph 2.3.
(8)	Failure effects given for the highest system level on the FMEA.
(9)	The source of reliability information used for each calculation should be identified in this column.
(10) - (16)	Enter the information required for the calculation of the portion of the component's criticality number due to each of its critical failure modes.
(17)	Enter the component's criticality numbers in this column. This is the sum of the portions of the criticality number entered in column (16) due to a particular mission phase and loss statement.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

System _____ Subsystem _____		Page _____ of _____ Pages Date _____ By _____		CRITICALITY ANALYSIS		Criticality Evaluation		(17) Component Criticality Number, C_r	
						(16) Critical Failure Mode Contribution			
						(15) Operating Time Hours or Cycles t			
						(14) Generic Failure Rate Failures/Hour or Cycle λ_G			
						(13) Operational Ratio K_A			
						(12) Environmental Ratio K_E			
						(11) Failure Mode Ratio α			
						(10) Probability of Failure Effects β			
						(9) Reliability Data Source Code			
						(8) Failure Effects			
						(7) Mission Phase			
						(6) Failure Mode and Cause			
						(5) Function			
						(4) Rel. Logic Diagram Number/Function Number			
						(3) Drawing Reference Designation			
						(2) Identification Number			
						(1) Name			

Figure E3 General Format for Criticality Number Calculation

4.0 SUMMARY OF FMECA AND CA**4.1 PREPARATION OF FMECA SUMMARY**

The procedure is a method for combining the criticality values by mission phase to develop an overall summary.

Preparation of the FMECA summary is developed from the FMEA and CA analysis discussed in Sections 2 and 3 and is accomplished by completing a form similar to that given in Figure E-4. Instructions for completing the form are given below.

A criticality list is prepared. Critical system components are grouped according to loss statement and are listed in the groups in descending order according to the magnitude of their total criticality number for the particular loss statement. A system component's total criticality number for a particular loss statement is computed from the FMECA summary information. Examples of ground rules for this are given below.

A general FMECA summary form is shown in Figure E-4. The columns are completed as follows:

<u>Column Number</u>	<u>Explanation or Description of Entries</u>
(1) - (5)	Identification and function of the system component with critical failure modes is the same as are those for the FMEA format in Figure E-1 which is described in Paragraph 2.3.
(6)	For each system component, enter its critical failure modes and, if known, their cause.
(7) - (9)	If the critical failure mode has an effect during Phase I of the mission, its effect on the system is given in Column (7) with mission time or event. The approved loss statement for the effect is given in Column (8). The portion of the total criticality number calculated for the critical failure mode according to the example given in Paragraph 3.3.1 is entered in Column (9).
(10) - (12)	Where the critical failure mode has an effect during Phase 2 of the mission, Columns (10)-(12) are completed in the same manner as in Columns (7)-(9). This format should be extended to include all mission phases.
(13)	A total criticality number may be computed for each system component according to approved ground rules. An example of ground rules is as follows:

USE FOR TYPEWRITTEN MATERIAL ONLY

4.1 (Continued)

Column
NumberExplanation or Description of Entries(13)
Contd.

- a. Each criticality number in the mission phase columns shall be multiplied by an approved importance weighting factor for its particular loss statement.

Example for stage/module level FMECA: Kills Crew = 1.0, Damages Vehicle = 0.5, Precludes Escape = 0.4, Loses Protective Devices = 0.3.

Example for subsystem level FMECA: Loss of critical output or input which could lead to crew loss = 1.0, Loss of noncritical input or output = 0.2, Annoyance failure = 0.1.

These examples are given only to convey the intent. A lengthy list of statements of actual loss may be ranked in relative importance by this means.

- b. A given critical failure mode in a system component shall occur only once during the mission, assuming no repair; therefore, the largest weighted criticality number for a critical failure mode will be selected from among the mission phase columns for calculation of the component's total criticality number.
- c. A component's total criticality number for a particular loss statement shall be the sum of the weighted criticality numbers with the same loss statement selected from the mission phase columns according to ground rule b, preceding.
- d. Each total criticality number with loss statement for a system component as calculated by ground rule c, above, shall be entered in Column (13) of the FMECA summary format.

4.2 CRITICALITY LIST

The last step of the FMECA is the preparation of the criticality list. Critical system components are grouped according to loss statement and are listed in the groups in descending order according to magnitude of their total criticality number for the loss statement. A system component may appear in more than one of the groups. Appropriate supporting information and recommendations should be given for each of the listed components.

USE FOR TYPEWRITTEN MATERIAL ONLY

USE FOR TYPEWRITTEN MATERIAL ONLY

<p>FMECA SUMMARY</p> <p>System _____</p> <p>Subsystem _____</p> <p>Page <u> </u> of <u> </u> Pages</p> <p>Date <u> </u> By <u> </u></p>		(13) System Component Total Criticality No.				
		Mission Phase Criticality		Phase 2	(12) Criticality Number	
					(11) Loss Statement	
					(10) Failure Effect	
		Phase 1		(9) Criticality Number		
				(8) Loss Statement		
				(7) Failure Effect		
		(6) Failure Mode and Cause				
		(5) Function				
		Item Identification		(4) Reliability Logic Diagram Number/Function Number		
(3) Drawing Reference Designation						
(2) Identification Number						
(1) Name						

Figure E4 General FMECA Summary Format

LIMITATIONS

This document is controlled by 5-8231 KSC TIE System Safety

All revisions to this document shall be approved by the
above noted organization prior to release.

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS				SHEET NUMBER	REV LTR	ADDED SHEETS			
		SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR			SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
1						4-15					
2						4-16					
3						4-17					
4						4-18					
5						4-19					
6						4-20					
7						4-21					
8						4-22					
1-0						4-23					
1-1						4-24					
1-2						4-25					
1-3						4-26					
1-4						4-27					
1-5						5-0					
2-0						5-1					
2-1						6-0					
2-2						6-1					
2-3						6-2					
2-4						6-3					
2-5						6-4					
2-6						6-5					
3-0						6-6					
3-1						6-7					
3-2						6-8					
3-3						A-001					
3-4						A-002					
3-5						A-101					
3-6						A-201					
3-7						A-301					
3-8						A-401					
4-0						A-402					
4-1						A-4C3					
4-2						A-501					
4-3						A-502					
4-4						B-001					
4-5						B-002					
4-6						B-003					
4-7						BI-101					
4-8						BI-102					
4-9						BI-201					
4-10						BI-301					
4-11						BI-302					
4-12						BI-303					
4-13						BI-304					
4-14											

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS				SHEET NUMBER	REV LTR	ADDED SHEETS			
		SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR			SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
BI-305						C-209					
BI-306						C-210					
BI-307						C-211					
BI-308						C-212					
BI-309						C-213					
BI-310						C-214					
BI-311						C-215					
BI-401						C-216					
BI-402						C-217					
BII-100						C-218					
BII-101						C-219					
BII-102						C-220					
BII-103						C-221					
BII-104						C-222					
BII-105						C-223					
BII-106						C-224					
BII-201						C-225					
BII-202						C-226					
BII-203						C-227					
BII-204						C-228					
BII-205						C-229					
BII-206						C-230					
BII-207						C-231					
BII-208						C-232					
BII-209						C-233					
BII-210						C-234					
C-001						C-235					
C-002						C-236					
C-003						C-237					
C-101						C-238					
C-102						C-239					
C-103						C-240					
C-104						C-241					
C-105						C-242					
C-106						C-243					
C-201						C-244					
C-202						C-245					
C-203						C-246					
C-204						C-247					
C-205						C-248					
C-206						C-249					
C-207						C-250					
C-208						C-251					
						C-252					
						C-253					
						C-254					

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS				SHEET NUMBER	REV LTR	ADDED SHEETS			
		SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR			SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
D-001											
D-002						E-401					
D-101						E-402					
D-102						E-403					
D-201						1001					
D-202						1002					
D-203						1003					
D-301						1004					
D-302						1005					
D-303											
D-304											
D-401											
D-501											
D-502											
D-503											
D-504											
D-505											
D-506											
D-507											
D-508											
D-509											
D-510											
D-511											
D-512											
E-001											
E-002											
E-003											
E-101											
E-102											
E-103											
E-201											
E-202											
E-203											
E-204											
E-205											
E-206											
E-207											
E-208											
E-301											
E-302											
E-303											
E-304											
E-305											
E-306											

REVISIONS			
LTR	DESCRIPTION	DATE	APPROVAL
	Original Release	6-30-69	
	Doc Control	6-30-69	MB